

NEW EQUIDISTRIBUTION ESTIMATES OF ZHANG TYPE

D.H.J. POLYMATH

ABSTRACT. We prove distribution estimates for primes in arithmetic progressions to large smooth squarefree moduli, with respect to congruence classes obeying Chinese Remainder Theorem conditions, obtaining an exponent of distribution $\frac{1}{2} + \frac{7}{300}$.

CONTENTS

1. Introduction	1
2. Preliminaries	8
3. Applying the Heath-Brown identity	14
4. One-dimensional exponential sums	23
5. Type I and Type II estimates	38
6. Trace functions and multidimensional exponential sum estimates	59
7. The Type III estimate	82
8. An improved Type I estimate	94
References	105

1. INTRODUCTION

In May 2013, Y. Zhang [52] proved the existence of infinitely many pairs of primes with bounded gaps. In particular, he showed that there exists at least one $h \geq 2$ such that the set

$$\{p \text{ prime} \mid p + h \text{ is prime}\}$$

is infinite. (In fact, he showed this for some even h between 2 and 7×10^7 , although the precise value of h could not be extracted from his method.)

Zhang's work started from the method of Goldston, Pintz and Yıldırım [23], who had earlier proved the bounded gap property, conditionally on distribution estimates concerning primes in arithmetic progressions to *large moduli*, i.e., beyond the reach of the Bombieri–Vinogradov theorem.

Based on work of Fouvry and Iwaniec [11, 12, 13, 14] and Bombieri, Friedlander and Iwaniec [3, 4, 5], distribution estimates going beyond the Bombieri–Vinogradov range for arithmetic functions such as the von Mangoldt function were already known. However, they involved restrictions concerning the residue classes which were incompatible with the method of Goldston, Pintz and Yıldırım.

Zhang's resolution of this difficulty proceeded in two stages. First, he isolated a weaker distribution estimate that sufficed to obtain the bounded gap property (still

involving the crucial feature of going beyond the range accessible to the Bombieri–Vinogradov technique), where (roughly speaking) only smooth¹ moduli were involved, and the residue classes had to obey strong multiplicative constraints (the possibility of such a weakening had been already noticed by Motohashi and Pintz [43]). Secondly, and more significantly, Zhang then proved such a distribution estimate.

This revolutionary achievement led to a flurry of activity. In particular, the POLYMATH8 project was initiated by T. Tao with the goal first of understanding, and then of improving and streamlining, where possible, the argument of Zhang. This was highly successful, and through the efforts of a number of people, reached a state in October 2013, when the first version of this paper [46] established the bounded gap property in the form

$$\liminf(p_{n+1} - p_n) \leq 4680,$$

where p_n denotes the n -th prime number.

However, at that time, J. Maynard [38] obtained another conceptual breakthrough, by showing how a modification of the structure and of the main term analysis of the method of Goldston, Pintz and Yıldırım was able to establish not only the bounded gap property using only the Bombieri–Vinogradov theorem (in fact the bound

$$\liminf(p_{n+1} - p_n) \leq 600$$

obtained was significantly better than the one obtained by POLYMATH8), but also the bounds

$$\liminf(p_{n+k} - p_n) < +\infty$$

for any fixed $k \geq 1$ (in a quantitative way), something which was out of reach of the earlier methods, even for $k = 2$. (Similar results were obtained independently in unpublished work of T. Tao.)

Because of this development, a part of the POLYMATH8 paper became essentially obsolete. Nevertheless, the distribution estimate for primes in arithmetic progressions are not superseded by the new method, and it has considerable interest for analytic number theory. Indeed, it is the best known result concerning primes in arithmetic progressions to large moduli without fixing the residue class. (When the class is fixed, the best results remain those of Bombieri, Friedlander and Iwaniec, improving on those of Fouvry and Iwaniec [13, 3].) The results here are also needed to obtain the best known bounds on $\liminf(p_{n+k} - p_n)$ for large values of k ; see [47].

The present version of the work of POLYMATH8 therefore contains only the statement and proof of these estimates. We note however that some of the earlier version is incorporated in our subsequent paper [47], which builds on Maynard’s method to further improve many bounds concerning gaps between primes, both conditional and unconditional. Furthermore, the original version of this paper, and the history of its elaboration, remain available online [46].

Our main theorem is:

Theorem 1.1. *Let $\theta = 1/2 + 7/300$. Let $\varepsilon > 0$ and $A \geq 1$ be fixed real numbers. For all primes p , let a_p be a fixed invertible residue class modulo p , and for $q \geq 1$ squarefree, denote by a_q the unique invertible residue class modulo q such that $a_q \equiv a_p$ modulo all primes p dividing q .*

¹ I.e., friable.

There exists $\delta > 0$, depending only on ε , such that for $x \geq 1$, we have

$$\sum_{\substack{q \leq x^{\theta-\varepsilon} \\ q \text{ } x^\delta\text{-smooth, squarefree}}} \left| \psi(x; q, a_q) - \frac{x}{\varphi(q)} \right| \ll \frac{x}{(\log x)^A},$$

where the implied constant depends only on A , ε and δ , and in particular is independent of the residue classes (a_p) .

In this statement, we have, as usual, defined

$$\psi(x; q, a) = \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} \Lambda(n),$$

where Λ is the von Mangoldt function. In [52], Zhang establishes a weaker form of Theorem 1.1, with $\theta = 1/2 + 1/584$, and with the a_q required to be roots of a polynomial P of the form $P(n) := \prod_{1 \leq j \leq k; j \neq i} (n + h_j - h_i)$ for a fixed admissible tuple (h_1, \dots, h_k) and $i = 1, \dots, k$.

In fact, we will prove a number of variants of this bound. These involve either weaker restrictions on the moduli (“dense-divisibility”, instead of smoothness, which may be useful in some applications), or smaller values of $\theta > 1/2$, but with significantly simpler proofs. In particular, although the full strength of Theorem 1.1 depends in crucial ways on applications of Deligne’s deepest form of the Riemann Hypothesis over finite fields, we show that, for a smaller value of $\theta > 1/2$, it is possible to obtain the same estimate by means of Weil’s theory of exponential sums in one variable over finite fields.

The outline of this paper is as follows: in the next section, we briefly outline the strategy, starting from the work of Bombieri, Fouvry, Friedlander, and Iwaniec (in chronological order, [12, 13, 21, 3, 4, 5, 14]), and explaining Zhang’s innovations. These involve different types of estimates of bilinear or trilinear nature, which we present in turn. All involve estimates for exponential sums over finite fields. We therefore survey the relevant theory, separating that part depending only on one-variable character sums of Weil type (Section 4), and the much deeper one which depends on Deligne’s form of the Riemann Hypothesis (Section 6). In both cases, we present the formalism in sometimes greater generality than strictly needed, as these results are of independent interest and might be useful for other applications.

1.1. Overview of proof. We begin with a brief and informal overview of the methods used in this paper.

Important work of Fouvry and Iwaniec [12, 13] and of Bombieri, Friedlander and Iwaniec [3, 4, 5] had succeeded, in some cases, in establishing distribution results similar to Theorem 1.1, in fact with θ as large as $1/2 + 1/14$, but with the restriction that the residue classes a_p are obtained by reduction modulo p of a fixed integer $a \geq 1$.

Following the techniques of Bombieri, Fouvry, Friedlander and Iwaniec, Zhang used the Heath-Brown identity [26] to reduce the proof of (his version of) Theorem 1.1 to the verification of three families of estimates, which he called “Type I”, “Type II”, and “Type III”. These estimates were then reduced to exponential sum estimates, using techniques such as Linnik’s dispersion method, completion of sums, and Weyl differencing. Ultimately, the exponential sum estimates were established by applications of the Riemann Hypothesis over finite fields, in analogy with all previous works of this type. The final part of Zhang’s argument is closely related to the study of the distribution of

the ternary divisor function in arithmetic progressions by Friedlander and Iwaniec [21], and indeed the final exponential sum estimate that Zhang uses already appears in their work (this estimate was proved by Birch and Bombieri in the Appendix to [21]). An important point is that, by using techniques that are closer to some older work of Fouvry and Iwaniec [12], Zhang avoids using the spectral theory of automorphic forms, which is a key ingredient in [13] and [3], and one of the sources of the limitation to a fixed residue in these works.

Our proof of Theorem 1.1 follows the same general strategy as Zhang’s, with improvements and refinements.

First, we apply the Heath-Brown identity [26] in Section 3, with little change compared with Zhang’s argument, reducing to the “bilinear” (Types I/II) and “trilinear” (Type III) estimates.

For the Type I and Type II estimates, we follow the arguments of Zhang to reduce to the task of bounding incomplete exponential sums similar to

$$\sum_{N < n \leq 2N} e\left(\frac{c_1 \bar{n} + c_2 \overline{n+l}}{q}\right),$$

(where $e(z) = e^{2i\pi z}$ and \bar{x} denotes the inverse of x modulo q) for various parameters N, c_1, c_2, l, q . We obtain significant improvements of Zhang’s numerology at this stage, by exploiting the smooth (or at least densely divisible) nature of q , using the q -van der Corput A -process of Heath-Brown [25] and Graham-Ringrose [24], combined with the Riemann Hypothesis for curves over finite fields. Additional gains are obtained by optimizing the parameterizations of sums prior to application of the Cauchy-Schwarz inequality. In our strongest Type I estimate, we also exploit additional averaging over the modulus by means of higher-dimensional exponential sum estimates, which now do depend on the deep results of Deligne. We refer to Sections 4, 5 and 8 for details of these parts of the arguments.

Finally, for the Type III sums, Zhang’s delicate argument [52] adapts and improves the work of Friedlander and Iwaniec [21] on the ternary divisor function in arithmetic progressions. As we said, it ultimately relies on a three-variable exponential sum estimate that was proved by Birch and Bombieri in the Appendix to [21]. Here, we proceed slightly differently, inspired by the streamlined approach of Fouvry, Kowalski, and Michel [16]. Namely, in Section 7 we show how our task can be reduced to obtaining certain correlation bounds on hyper-Kloosterman sums. These bounds are established in Section 6, by fully exploiting the formalism of “trace functions” over finite fields (which relies on Deligne’s second, more general proof of the Riemann Hypothesis over finite fields [9]). The very general techniques presented in Section 6 are also used in the proof of the strongest Type I estimate in Section 8, and we present them in considerable detail in order to make them more accessible to analytic number theorists.

1.2. About this project. This paper is part of the *Polymath project*, which was launched by Timothy Gowers in February 2009 as an experiment to see if research mathematics could be conducted by a massive online collaboration. The current project (which was administered by Terence Tao) is the eighth project in this series. Further information on the Polymath project can be found on the web site michaelnielsen.org/polymath1. Information about this specific project may be found at

michaelnielsen.org/polymath1/index.php?title=Bounded_gaps_between_primes

and a full list of participants and their grant acknowledgments may be found at michaelnielsen.org/polymath1/index.php?title=Polymath8_grant_acknowledgments

We thank John Friedlander for help with the references. We are indebted to the multiple referees of the first version of this paper for many cogent suggestions and corrections.

1.3. Basic notation. We use $|E|$ to denote the cardinality of a finite set E , and $\mathbf{1}_E$ to denote the indicator function of a set E , thus $\mathbf{1}_E(n) = 1$ when $n \in E$ and $\mathbf{1}_E(n) = 0$ otherwise.

All sums and products will be over the natural numbers $\mathbb{N} := \{1, 2, 3, \dots\}$ unless otherwise specified, with the exceptions of sums and products over the variable p , which will be understood to be over primes.

The following important asymptotic notation will be in use throughout most of the paper; when it is not (as in Section 6), we will mention this explicitly.

Definition 1.2 (Asymptotic notation). We use x to denote a large real parameter, which one should think of as going off to infinity; in particular, we will implicitly assume that it is larger than any specified fixed constant. Some mathematical objects will be independent of x and referred to as *fixed*; but unless otherwise specified we allow all mathematical objects under consideration to depend on x (or to vary within a range that depends on x , e.g. the summation parameter n in the sum $\sum_{x \leq n \leq 2x} f(n)$). If X and Y are two quantities depending on x , we say that $X = O(Y)$ or $X \ll Y$ if one has $|X| \leq CY$ for some fixed C (which we refer to as the *implied constant*), and $X = o(Y)$ if one has $|X| \leq c(x)Y$ for some function $c(x)$ of x (and of any fixed parameters present) that goes to zero as $x \rightarrow \infty$ (for each choice of fixed parameters). We use $X \ll Y$ to denote the estimate $X \leq x^{o(1)}Y$, $X \asymp Y$ to denote the estimate $Y \ll X \ll Y$, and $X \approx Y$ to denote the estimate $Y \ll X \ll Y$. Finally, we say that a quantity n is of *polynomial size* if one has $n = O(x^{O(1)})$.

If asymptotic notation such as $O()$ or \ll appears on the left-hand side of a statement, this means that the assertion holds true for any specific interpretation of that notation. For instance, the assertion $\sum_{n=O(N)} |\alpha(n)| \ll N$ means that for each fixed constant $C > 0$, one has $\sum_{|n| \leq CN} |\alpha(n)| \ll N$.

If q and a are integers, we write $a|q$ if a divides q .

If q is a natural number and $a \in \mathbb{Z}$, we use $a \pmod{q}$ to denote the congruence class

$$a \pmod{q} := \{a + nq : n \in \mathbb{Z}\}$$

and let $\mathbb{Z}/q\mathbb{Z}$ denote the ring of all such congruence classes $a \pmod{q}$. The notation $b = a \pmod{q}$ is synonymous to $b \in a \pmod{q}$. We use (a, q) to denote the greatest common divisor of a and q , and $[a, q]$ to denote the least common multiple.² More generally, we let (q_1, \dots, q_k) denote the greatest simultaneous common divisor of q_1, \dots, q_k . We note in particular that $(0, q) = q$ for any natural number q . Note that $a \mapsto (a, q)$ is periodic with period q , and so we may also define (a, q) for $a \in \mathbb{Z}/q\mathbb{Z}$ without ambiguity. We also let

$$(\mathbb{Z}/q\mathbb{Z})^\times := \{a \pmod{q} : (a, q) = 1\}$$

²When a, b are real numbers, we will also need to use (a, b) and $[a, b]$ to denote the open and closed intervals respectively with endpoints a, b . Unfortunately, this notation conflicts with the notation given above, but it should be clear from the context which notation is in use. Similarly for the notation \bar{a} for $a \in \mathbb{Z}/q\mathbb{Z}$, and the notation \bar{z} to denote the complex conjugate of a complex number z .

denote the primitive congruence classes of $\mathbb{Z}/q\mathbb{Z}$. More generally, for any commutative ring R (with unity) we use R^\times to denote the multiplicative group of units. If $a \in (\mathbb{Z}/q\mathbb{Z})^\times$, we use \bar{a} to denote the inverse of a in $\mathbb{Z}/q\mathbb{Z}$.

For any real number x , we write $e(x) := e^{2\pi i x}$. We denote $e_q(a) := e(\frac{a}{q}) = e^{2\pi i a/q}$ (see also the conventions concerning this additive character at the beginning of Section 4).

We use the following standard arithmetic functions:

- (i) $\varphi(q) := |(\mathbb{Z}/q\mathbb{Z})^\times|$ denotes the Euler totient function of q .
- (ii) $\tau(q) := \sum_{d|q} 1$ denotes the divisor function of q .
- (iii) $\Lambda(q)$ denotes the von Mangoldt function of q , thus $\Lambda(q) = \log p$ if q is a power of a prime p , and $\Lambda(q) = 0$ otherwise.
- (iv) $\theta(q)$ is defined to equal $\log q$ when q is a prime, and $\theta(q) = 0$ otherwise.
- (v) $\mu(q)$ denotes the Möbius function of q , thus $\mu(q) = (-1)^k$ if q is the product of k distinct primes for some $k \geq 0$, and $\mu(q) = 0$ otherwise.
- (vi) $\Omega(q)$ denotes the number of prime factors of q (counting multiplicity).

The *Dirichlet convolution* $\alpha \star \beta: \mathbb{N} \rightarrow \mathbb{C}$ of two arithmetic functions $\alpha, \beta: \mathbb{N} \rightarrow \mathbb{C}$ is defined in the usual fashion as

$$\alpha \star \beta(n) := \sum_{d|n} \alpha(d) \beta\left(\frac{n}{d}\right) = \sum_{ab=n} \alpha(a) \beta(b).$$

Many of the key ideas in Zhang's work (as well as in the present article) concern the uniform distribution of arithmetic functions in arithmetic progressions. For any function $\alpha: \mathbb{N} \rightarrow \mathbb{C}$ with finite support (that is, α is non-zero only on a finite set) and any primitive congruence class $a \pmod{q}$, we define the (signed) *discrepancy* $\Delta(\alpha; a \pmod{q})$ to be the quantity

$$\Delta(\alpha; a \pmod{q}) := \sum_{n=a \pmod{q}} \alpha(n) - \frac{1}{\varphi(q)} \sum_{(n,q)=1} \alpha(n). \quad (1.1)$$

There are some additional concepts and terminology that will be used in multiple sections of this paper. These are listed in Table 1.

We will often use the following simple estimates for the divisor function τ and its powers.

Lemma 1.3 (Crude bounds on τ).

(i) (*Divisor bound*) One has

$$\tau(d) \ll 1 \quad (1.2)$$

whenever d is of polynomial size. In particular, d has $o(\log x)$ distinct prime factors.

(ii) One has

$$\sum_{d \leq y} \tau^C(d) \ll y \log^{O(1)} x \quad (1.3)$$

for any fixed $C > 0$ and any $y > 1$ of polynomial size.

(iii) More generally, one has

$$\sum_{\substack{d \leq y \\ d \equiv a \pmod{q}}} \tau^C(d) \ll \frac{y}{q} \tau^{O(1)}(q) \log^{O(1)} x + x^{o(1)} \quad (1.4)$$

for any fixed $C > 0$, any residue class $a \pmod{q}$ (not necessarily primitive), and any $y > 1$ of polynomial size.

TABLE 1: Notation and terminology

ϖ	Level of distribution	§2
δ	Smoothness/dense divisibility parameter	§2
i	Multiplicity of dense divisibility	Definition 2.1
σ	Type I/III boundary parameter	Definition 2.6
$\text{MPZ}^{(i)}[\varpi, \delta]$	MPZ conjecture for densely divisible moduli	Claim 2.3
$\text{Type}_I^{(i)}[\varpi, \delta, \sigma]$	Type I estimate	Definition 2.6
$\text{Type}_{II}^{(i)}[\varpi, \delta]$	Type II estimate	Definition 2.6
$\text{Type}_{III}^{(i)}[\varpi, \delta, \sigma]$	Type III estimate	Definition 2.6
\mathcal{S}_I	Squarefree products of primes in I	Definition 2.2
P_I	Product of all primes in I	Definition 2.2
$\mathcal{D}^{(i)}(y)$	i -tuply y -densely divisible integers	Definition 2.1
$\text{FT}_q(f)$	Normalized Fourier transform of f	(4.11)
	Coefficient sequence at scale N	Definition 2.5
	Siegel-Walfisz theorem	Definition 2.5
	(Shifted) smooth sequence at scale N	Definition 2.5

Proof. For the divisor bound (1.2), see e.g. [40, Theorem 2.11]. For the bound (1.3), see e.g. [40, Corollary 2.15]. Finally, to prove the bound (1.4), observe using (1.2) that we may factor out any common factor of a and q , so that $a(q)$ is primitive. Next, we may assume that $q \leq y$, since the case $q > y$ is trivial by (1.2). The claim now follows from the Brun-Titchmarsh inequality for multiplicative functions (see [48] or [1]). \square

Note that we have similar bounds for the higher divisor functions

$$\tau_k(n) := \sum_{d_1, \dots, d_k: d_1 \dots d_k = n} 1$$

for any fixed $k \geq 2$, thanks to the crude upper bound $\tau_k(n) \leq \tau(n)^{k-1}$.

The following elementary consequence of the divisor bound will also be useful:

Lemma 1.4. *Let $q \geq 1$ be an integer. Then for any $K \geq 1$ we have*

$$\sum_{1 \leq k \leq K} (k, q) \leq K\tau(q).$$

In particular, if q is of polynomial size, then we have

$$\sum_{a \in \mathbb{Z}/q\mathbb{Z}} (a, q) \ll q,$$

and we also have

$$\sum_{|k| \leq K} (k, q) \ll Kq^\varepsilon + q$$

for any fixed $\varepsilon > 0$ and arbitrary q (not necessarily of polynomial size).

Proof. We have

$$(k, q) \leq \sum_{d|(q,k)} d$$

and hence

$$\sum_{1 \leq k \leq K} (k, q) \leq \sum_{d|q} \sum_{\substack{1 \leq k \leq K \\ d|k}} d \leq K\tau(q).$$

□

2. PRELIMINARIES

2.1. Statements of results. In this section we will give the most general statements that we prove, and in particular define the concept of “dense divisibility”, which weakens the smoothness requirement of Theorem 1.1.

Definition 2.1 (Multiple dense divisibility). Let $y \geq 1$. For each natural number $i \geq 0$, we define a notion of i -tuply y -dense divisibility recursively as follows:

- (i) Every natural number n is 0-tuply y -densely divisible.
- (ii) If $i \geq 1$ and n is a natural number, we say that n is i -tuply y -densely divisible if, whenever $j, k \geq 0$ are natural numbers with $j + k = i - 1$, and $1 \leq R \leq yn$, one can find a factorisation

$$n = qr, \quad \text{with } y^{-1}R \leq r \leq R \quad (2.1)$$

such that q is j -tuply y -densely divisible and r is k -tuply y -densely divisible.

We let $\mathcal{D}^{(i)}(y)$ denote the set of i -tuply y -densely divisible numbers. We abbreviate “1-tuply densely divisible” as “densely divisible”, “2-tuply densely divisible” as “doubly densely divisible”, and so forth; we also abbreviate $\mathcal{D}^{(1)}(y)$ as $\mathcal{D}(y)$, and since we will often consider squarefree densely divisible integers with prime factors in an interval I , we will denote

$$\mathcal{D}_I^{(j)}(y) = \mathcal{S}_I \cap \mathcal{D}^{(j)}(y). \quad (2.2)$$

A number of basic properties of this notion will be proved at the beginning of Section 2.3, but the intent is that we want to have integers which can always be factored, in such a way that we can control the location of the divisors. For instance, the following fact is quite easy to check: any y -smooth integer is also i -tuply y -densely divisible, for any $i \geq 0$ (see Lemma 2.10 (iii) for details).

Definition 2.2. For any set $I \subset \mathbb{R}$ (possibly depending on x), let \mathcal{S}_I denote the set of all squarefree natural numbers whose prime factors lie in I . If I is also a bounded set (with the bound allowed to depend on x), we let P_I denote the product of all the primes in I , thus in this case \mathcal{S}_I is the set of divisors of P_I .

For every fixed $0 < \varpi < \frac{1}{4}$ and $0 < \delta < \frac{1}{4} + \varpi$ and every natural number i , we let $\text{MPZ}^{(i)}[\varpi, \delta]$ denote the following claim:

Claim 2.3 (Modified Motohashi-Pintz-Zhang estimate, $\text{MPZ}^{(i)}[\varpi, \delta]$). *Let $I \subset \mathbb{R}$ be a bounded set, which may vary with x , and let $Q \ll x^{1/2+2\varpi}$. If a is an integer coprime to P_I , and $A \geq 1$ is fixed, then*

$$\sum_{\substack{q \leq Q \\ q \in \mathcal{D}_I^{(i)}(x^\delta)}} |\Delta(\Lambda \mathbf{1}_{[x, 2x]}; a(q))| \ll x \log^{-A} x. \quad (2.3)$$

We will prove the following cases of these estimates:

Theorem 2.4 (Motohashi-Pintz-Zhang type estimates).

- (i) We have $\text{MPZ}^{(4)}[\varpi, \delta]$ for any fixed $\varpi, \delta > 0$ such that $600\varpi + 180\delta < 7$.
- (ii) We can prove $\text{MPZ}^{(2)}[\varpi, \delta]$ for any fixed $\varpi, \delta > 0$ such that $168\varpi + 48\delta < 1$, without invoking any of Deligne's results [8, 9] on the Riemann Hypothesis over finite fields.

The statement $\text{MPZ}^{(i)}[\varpi, \delta]$ is easier to establish as i increases. If true for some $i \geq 1$, it implies

$$\sum_{\substack{q \leq x^{1/2+2\varpi-\varepsilon} \\ q \text{ } x^\delta\text{-smooth, squarefree}}} |\Delta(\Lambda \mathbf{1}_{[x, 2x]}; a(q))| \ll x \log^{-A} x$$

for any $A \geq 1$ and $\varepsilon > 0$. Using a dyadic decomposition and the Chinese Remainder Theorem, this shows that Theorem 2.4 (i) implies Theorem 1.1.

2.2. Bilinear and trilinear estimates. As explained, we will reduce Theorem 2.4 to bilinear or trilinear estimates. In order to state these precisely, we introduce some further notation.

Definition 2.5 (Coefficient sequences). A *coefficient sequence* is a finitely supported sequence $\alpha: \mathbb{N} \rightarrow \mathbb{R}$ (which may depend on x) that obeys the bounds

$$|\alpha(n)| \ll \tau^{O(1)}(n) \log^{O(1)}(x) \quad (2.4)$$

for all n (recall that τ is the divisor function).

- (i) A coefficient sequence α is said to be *located at scale N* for some $N \geq 1$ if it is supported on an interval of the form $[cN, CN]$ for some $1 \ll c < C \ll 1$.
- (ii) A coefficient sequence α located at scale N for some $N \geq 1$ is said to *obey the Siegel-Walfisz theorem*, or to *have the Siegel-Walfisz property*, if one has

$$|\Delta(\alpha \mathbf{1}_{(\cdot, r)=1}; a(q))| \ll \tau(qr)^{O(1)} N \log^{-A} x \quad (2.5)$$

for any $q, r \geq 1$, any fixed A , and any primitive residue class $a(q)$.

- (iii) A coefficient sequence α is said to be *shifted smooth at scale N* for some $N \geq 1$ if it has the form $\alpha(n) = \psi(\frac{n-x_0}{N})$ for some smooth function $\psi: \mathbb{R} \rightarrow \mathbb{C}$ supported on an interval $[c, C]$ for some fixed $0 < c < C$, and some real number x_0 , with ψ obeying the derivative bounds

$$|\psi^{(j)}(x)| \ll \log^{O(1)} x \quad (2.6)$$

for all fixed $j \geq 0$, where the implied constant may depend on j , and where $\psi^{(j)}$ denotes the j^{th} derivative of ψ . If we can take $x_0 = 0$, we call α *smooth at scale N* ; note that such sequences are also located at scale N .

Note that for a coefficient sequence α at scale N , an integer $q \geq 1$ and a primitive residue class $a(q)$, we have the trivial estimate

$$\Delta(\alpha; a(q)) \ll \frac{N}{\varphi(q)} (\log x)^{O(1)}. \quad (2.7)$$

In particular, we see that the Siegel-Walfisz property amounts to a requirement that the sequence α be uniformly equidistributed in arithmetic progressions to moduli $q \ll (\log x)^A$ for any A . In the most important arithmetic cases, it is established using the methods from the classical theory of L -functions.

Definition 2.6 (Type I,II,III estimates). Let $0 < \varpi < 1/4$, $0 < \delta < 1/4 + \varpi$, and $0 < \sigma < 1/2$ be fixed quantities, and let $i \geq 1$ be a fixed natural number. We let I be an arbitrary bounded subset of \mathbb{R} and define $P_I = \prod_{p \in I} p$ as before. Let $a(P_I)$ be a primitive congruence class.

- (i) We say that $\text{Type}_I^{(i)}[\varpi, \delta, \sigma]$ holds if, for any I and $a(P_I)$ as above, any quantities $M, N \gg 1$ with

$$MN \asymp x \quad (2.8)$$

and

$$x^{1/2-\sigma} \ll N \ll x^{1/2-2\varpi-c} \quad (2.9)$$

for some fixed $c > 0$, any $Q \ll x^{1/2+2\varpi}$, and any coefficient sequences α, β located at scales M, N respectively, with β having the Siegel-Walfisz property, we have

$$\sum_{\substack{q \leq Q \\ q \in \mathcal{D}_I^{(i)}(x^\delta)}} |\Delta(\alpha \star \beta; a(q))| \ll x \log^{-A} x \quad (2.10)$$

for any fixed $A > 0$. (Recall the definition (2.2) of the set $\mathcal{D}_I^{(i)}(x^\delta)$.)

- (ii) We say that $\text{Type}_{II}^{(i)}[\varpi, \delta]$ holds if, for any I and $a(P_I)$ as above, any quantities $M, N \gg 1$ obeying (2.8) and

$$x^{1/2-2\varpi-c} \ll N \ll x^{1/2} \quad (2.11)$$

for some sufficiently small fixed $c > 0$, any $Q \ll x^{1/2+2\varpi}$, and any coefficient sequences α, β located at scales M, N respectively, with β having the Siegel-Walfisz property, we have (2.10) for any fixed $A > 0$.

- (iii) We say that $\text{Type}_{III}^{(i)}[\varpi, \delta, \sigma]$ holds if, for any I and $a(P_I)$ as above, for any quantities $M, N_1, N_2, N_3 \gg 1$ which satisfy the conditions

$$MN_1N_2N_3 \asymp x$$

$$N_1N_2, N_1N_3, N_2N_3 \gg x^{1/2+\sigma} \quad (2.12)$$

$$x^{2\sigma} \ll N_1, N_2, N_3 \ll x^{1/2-\sigma}, \quad (2.13)$$

for any coefficient sequences $\alpha, \psi_1, \psi_2, \psi_3$ located at scales M, N_1, N_2, N_3 , respectively, with ψ_1, ψ_2, ψ_3 smooth, and finally for any $Q \ll x^{1/2+2\varpi}$, we have

$$\sum_{\substack{q \leq Q \\ q \in \mathcal{D}_I^{(i)}(x^\delta)}} |\Delta(\alpha \star \psi_1 \star \psi_2 \star \psi_3; a(q))| \ll x \log^{-A} x \quad (2.14)$$

for any fixed $A > 0$.

Roughly speaking, Type I estimates control the distribution of Dirichlet convolutions α, β where α, β are rough coefficient sequences at moderately different scales, Type II estimates control the distribution of Dirichlet convolutions α, β where α, β are rough coefficient sequences at almost the same scale, and Type III estimates control the distribution of Dirichlet convolutions $\alpha \star \psi_1 \star \psi_2 \star \psi_3$ where ψ_1, ψ_2, ψ_3 are smooth and α is rough but supported at a fairly small scale.

In Section 3, we will use the Heath-Brown identity to reduce $\text{MPZ}^{(i)}[\varpi, \delta]$ to a combination of $\text{Type}_I^{(i)}[\varpi, \delta, \sigma]$, $\text{Type}_{II}^{(i)}[\varpi, \delta]$, and $\text{Type}_{III}^{(i)}[\varpi, \delta, \sigma]$:

Lemma 2.7 (Combinatorial lemma). *Let $i \geq 1$ be a fixed integer, and let $0 < \varpi < \frac{1}{4}$, $0 < \delta < \frac{1}{4} + \varpi$, and $\frac{1}{10} < \sigma < \frac{1}{2}$ be fixed quantities with $\sigma > 2\varpi$, such that the estimates $\text{Type}_I^{(i)}[\varpi, \delta, \sigma]$, $\text{Type}_{II}^{(i)}[\varpi, \delta]$, and $\text{Type}_{III}^{(i)}[\varpi, \delta, \sigma]$ all hold. Then $\text{MPZ}^{(i)}[\varpi, \delta]$ holds.*

Furthermore, if $\sigma > 1/6$, then the hypothesis $\text{Type}_{III}^{(i)}[\varpi, \delta, \sigma]$ may be omitted.

As stated earlier, this lemma is a simple consequence of the Heath-Brown identity, a dyadic decomposition (or more precisely, a finer-than-dyadic decomposition), some standard analytic number theory estimates (in particular, the Siegel-Walfisz theorem) and some elementary combinatorial arguments.

In Zhang's work [52], the claims $\text{Type}_I[\varpi, \delta, \sigma]$, $\text{Type}_{II}[\varpi, \delta]$, $\text{Type}_{III}[\varpi, \delta, \sigma]$ are (implicitly) proven with $\varpi = \delta = 1/1168$ and $\sigma = 1/8 - 8\varpi$. In fact, if one optimizes the numerology in his arguments, one can derive $\text{Type}_I[\varpi, \delta, \sigma]$ whenever $44\varpi + 12\delta + 8\sigma < 1$, $\text{Type}_{II}[\varpi, \delta]$ whenever $116\varpi + 20\delta < 1$, and $\text{Type}_{III}[\varpi, \delta, \sigma]$ whenever $\sigma > \frac{3}{26} + \frac{32}{13}\varpi + \frac{2}{13}\delta$ (see [45] for details). We will obtain the following improvements to these estimates, where the dependency with respect to σ is particularly important:

Theorem 2.8 (New Type I, II, III estimates). *Let $\varpi, \delta, \sigma > 0$ be fixed quantities.*

- (i) *If $54\varpi + 15\delta + 5\sigma < 1$, then $\text{Type}_I^{(1)}[\varpi, \delta, \sigma]$ holds.*
- (ii) *If $56\varpi + 16\delta + 4\sigma < 1$, then $\text{Type}_I^{(2)}[\varpi, \delta, \sigma]$ holds.*
- (iii) *If $\frac{160}{3}\varpi + 16\delta + \frac{34}{9}\sigma < 1$ and $64\varpi + 18\delta + 2\sigma < 1$, then $\text{Type}_I^{(4)}[\varpi, \delta, \sigma]$ holds.*
- (iv) *If $68\varpi + 14\delta < 1$, then $\text{Type}_{II}^{(1)}[\varpi, \delta]$ holds.*
- (v) *If $\sigma > \frac{1}{18} + \frac{28}{9}\varpi + \frac{2}{9}\delta$ and $\varpi < 1/12$, then $\text{Type}_{III}^{(1)}[\varpi, \delta, \sigma]$ holds.*

The proofs of the claims in (iii) and (v) require Deligne's work on the Riemann Hypothesis over finite fields, but the claims in (i), (ii) and (iv) do not.

In proving these estimates, we will rely on the following general “bilinear” form of the Bombieri-Vinogradov theorem (the principle of which is due to Gallagher [22] and Motohashi [42]).

Theorem 2.9 (Bombieri-Vinogradov theorem). *Let $N, M \gg 1$ be such that $NM \asymp x$ and $N \geq x^\varepsilon$ for some fixed $\varepsilon > 0$. Let α, β be coefficient sequences at scale M, N respectively such that β has the Siegel-Walfisz property. Then for any fixed $A > 0$ there exists a fixed $B > 0$ such that*

$$\sum_{q \leq x^{1/2} \log^{-B} x} \sup_{a \in (\mathbb{Z}/q\mathbb{Z})^\times} |\Delta(\alpha \star \beta; a(q))| \ll x \log^{-A} x.$$

See [3, Theorem 0] for the proof. Besides the assumption of the Siegel-Walfisz property, the other main ingredient used to establish Theorem 2.9 is the large sieve inequality for Dirichlet characters, from which the critical limitation to moduli less than $x^{1/2}$ arises.

The Type I and Type II estimates in Theorem 2.8 will be proven in Section 5, with the exception of the more difficult Type I estimate (iii) which is proven in Section 8. The Type III estimate is established in Section 7. In practice, the estimate in Theorem 2.8(i) gives inferior results to that in Theorem 2.8(ii), but we include it here because it has a slightly simpler proof.

The proofs of these estimates involve essentially all the methods that have been developed or exploited for the study of the distribution of arithmetic functions in arithmetic progressions to large moduli, for instance the dispersion method, completion of sums,

the Weyl differencing technique, and the q -van der Corput A process. All rely ultimately on some estimates of (incomplete) exponential sums over finite fields, either one-dimensional or higher-dimensional. These final estimates are derived from forms of the Riemann Hypothesis over finite fields, either in the (easier) form due to Weil [51], or in the much more general form due to Deligne [9].

2.3. Properties of dense divisibility. We present the most important properties of the notion of multiple dense divisibility, as defined in Definition 2.1. Roughly speaking, dense divisibility is a weaker form of smoothness which guarantees a plentiful supply of divisors of the given number in any reasonable range, and multiple dense divisibility is a hereditary version of this property which also partially extends to some factors of the original number.

Lemma 2.10 (Properties of dense divisibility). *Let $i \geq 0$ and $y \geq 1$.*

- (0) *If n is i -tuply y -densely divisible, and $y_1 \geq y$, then n is i -tuply y_1 -densely divisible. Furthermore, if $0 \leq j \leq i$, then n is j -tuply y -densely divisible.*
- (i) *If n is i -tuply y -densely divisible, and m is a divisor of n , then m is i -tuply $y(n/m)$ -densely divisible. Similarly, if l is a multiple of n , then l is i -tuply $y(l/n)$ -densely divisible.*
- (ii) *If m, n are y -densely divisible, then $[m, n]$ is also y -densely divisible.*
- (iii) *Any y -smooth number is i -tuply y -densely divisible.*
- (iv) *If n is z -smooth and squarefree for some $z \geq y$, and*

$$\prod_{\substack{p|n \\ p \leq y}} p \geq \frac{z^i}{y}, \quad (2.15)$$

then n is i -tuply y -densely divisible.

Proof. We abbreviate “ i -tuply y -divisible” in this proof by the shorthand “ (i, y) -d.d.”.

(0) These monotony properties are immediate from the definition.

Before we prove the other properties, we make the following remark: in checking that an integer n is (i, y) -d.d., it suffices to consider parameters R with $1 \leq R \leq n$ when looking for factorizations of the form (2.1): indeed, if $n < R \leq yn$, the factorization $n = qr$ with $r = n$ and $q = 1$ satisfies the condition $y^{-1}R \leq r \leq R$, and $r = n$ is (j, y) -d.d. (resp. $q = 1$ is (k, y) -d.d.) whenever $j + k = i - 1$. We will use this reduction in (i), (ii), (iii), (iv) below.

(i) We prove the first part by induction on i . For $i = 0$, the statement is obvious since every integer is $(0, y)$ -d.d. for every $y \geq 1$. Now assume the property holds for j -tuply dense divisibility for $j < i$, let n be (i, y) -d.d., and let $m \mid n$ be a divisor of n . We proceed to prove that m is (i, ym_1) -d.d.

We write $n = mm_1$. Let R be such that $1 \leq R \leq m$, and let $j, k \geq 0$ be integers with $j + k = i - 1$. Since $R \leq n$, and n is (i, y) -d.d., there exists by definition a factorization $n = qr$ where q is (j, y) -d.d., r is (k, y) -d.d., and $y/R \leq r \leq y$. Now we write $m_1 = n_1 n'_1$ where $n_1 = (r, m_1)$ is the gcd of r and m_1 . We have then a factorization $m = q_1 r_1$ where

$$q_1 = \frac{q}{n'_1}, \quad r_1 = \frac{r}{n_1},$$

and we check that this factorization satisfies the condition required for checking that m is (i, ym_1) -d.d. First, we have

$$\frac{R}{ym_1} \leq \frac{r}{m_1} \leq \frac{r}{n_1} = r_1 \leq R,$$

so the divisor r_1 is well-located. Next, by induction applied to the divisor $r_1 = r/n_1$ of the (k, y) -d.d. integer r , this integer is (k, yn_1) -d.d., and hence by (0), it is also (k, ym_1) -d.d. Similarly, q_1 is (j, yn'_1) -d.d., and hence also (j, ym_1) -d.d. This finishes the proof that m is (i, ym_1) -d.d.

The second part of (i) is similar and left to the reader.

To prove (ii), recall that y -densely divisible means $(1, y)$ -densely divisible. We may assume that $m \leq n$. Denote $a = [m, n]n^{-1}$. Now let R be such that $1 \leq R \leq [m, n]$. If $R \leq n$, then a factorization $n = qr$ with $Ry^{-1} \leq r \leq R$, which exists since n is y -d.d., gives the factorization $[m, n] = aqr$, which has the well-located divisor r . If $n < R \leq [m, n]$, we get

$$1 \leq \frac{n}{a} \leq \frac{R}{a} \leq n$$

and therefore there exists a factorization $n = qr$ with $R(ay)^{-1} \leq r \leq Ra^{-1}$. Then $[m, n] = q(ar)$ with $Ry^{-1} \leq ar \leq R$. Thus we see that $[m, n]$ is y -d.d.

We now prove (iii) by induction on i . The case $i = 0$ is again obvious, so we assume that (iii) holds for j -tuply dense divisibility for $j < i$. Let n be a y -smooth integer, let $j, k \geq 0$ satisfy $j + k = i - 1$, and let $1 \leq R \leq n$ be given. Let r be the largest divisor of n which is $\leq R$, and let $q = n/r$. Since all prime divisors of n are $\leq y$, we have

$$Ry^{-1} \leq r \leq R,$$

and furthermore both q and r are y -smooth. By the induction hypothesis, q is (j, y) -d.d. and r is (k, y) -d.d., hence it follows that n is (i, y) -d.d.

We now turn to (iv). The claim is again obvious for $i = 0$. Assume then that $i = 1$. Let R be such that $1 \leq R \leq n$. Let

$$s_1 = \prod_{\substack{p|n \\ p \leq y}} p, \quad r_1 = \prod_{\substack{p|n \\ p > y}} p.$$

Assume first that $r_1 \leq R$. Since $n/r_1 = s_1$ is y -smooth, it is 1-d.d., and since $1 \leq Rr_1^{-1} \leq s_1$, we can factor $s_1 = q_2r_2$ with $R(r_1y)^{-1} \leq r_2 \leq Rr_1^{-1}$. Then $n = q_2(r_1r_2)$ with

$$Ry^{-1} \leq r_1r_2 \leq R.$$

So assume that $r_1 > R$. Since n and hence r_1 are z -smooth, we can factor $r_1 = r_2q_2$ with $Rz^{-1} \leq r_2 \leq R$. Let r_3 be the smallest divisor of s_1 such that $r_3r_2 \geq Ry^{-1}$, which exists because $s_1r_2 \geq zy^{-1}r_2 \geq Ry^{-1}$ by the assumption (2.15). Since s_1 is y -smooth, we have $r_3r_2 \leq R$ (since otherwise we must have $r_3 \neq 1$, hence r_3 is divisible by a prime $p \leq y$, and r_3p^{-1} is a smaller divisor with the required property $r_3p^{-1}r_2 > Ry^{-1}$, contradicting the minimality of r_3). Therefore $n = q(r_3r_2)$ with

$$\frac{R}{y} \leq r_3r_2 \leq R,$$

as desired.

Finally we consider the $i > 1$ case. We assume, by induction, that (iv) holds for integers $j < i$. Let $j, k \geq 0$ be such that $j + k = i - 1$. By assumption, using the notation r_1, s_1 as above, we have

$$s_1 \geq z^i y^{-1} = z^j \cdot z^k \cdot \frac{z}{y}.$$

We can therefore write $s_1 = n_1 n_2 n_3$ where

$$z^j y^{-1} \leq n_1 \leq z^j, \quad z^k y^{-1} \leq n_2 \leq z^k \quad (2.16)$$

and thus

$$n_3 \geq \frac{z}{y}.$$

Now we divide into several cases in order to find a suitable factorization of n . Suppose first that $n_1 \leq R \leq n/n_2$. Then

$$1 \leq \frac{R}{n_1} \leq \frac{n}{n_1 n_2}$$

and the integer $n/(n_1 n_2) = r_1 n_3$ satisfies the assumptions of (iv) for $i = 1$. Thus, by the previous case, we can find a factorization $r_1 n_3 = q' r'$ with $y^{-1} \frac{R}{n_1} \leq r' \leq \frac{R}{n_1}$. We set $r = n_1 r'$ and $q = n_2 q'$, and observe that by (2.16), r (resp. q) satisfies the assumption of (iv) for $i = j$ (resp. $i = k$). By induction, the factorization $n = qr$ has the required property.

Next, we assume that $R < n_1$. Since n_1 is y -smooth, we can find a divisor r of n_1 such that $y^{-1} R \leq r \leq R$. Then $q = n/r$ is a multiple of n_2 , and therefore it satisfies

$$\prod_{\substack{p|q \\ p \leq y}} p \geq n_2 \geq z^k y^{-1}.$$

By induction, it follows that q is (k, y) -d.d. Since r is y -smooth, q is also (j, y) -d.d. by (iii), and hence the factorization $n = qr$ is suitable in this case.

Finally, suppose that $R > n/n_2$, i.e., that $nR^{-1} < n_2$. We then find a factor q of the y -smooth integer n_2 such that $n(Ry)^{-1} \leq q \leq nR^{-1}$. Then the complementary factor $r = n/q$ is a multiple of n_1 , and therefore it satisfies

$$\prod_{\substack{p|r \\ p \leq y}} p \geq z^j y^{-1},$$

so that r is (j, y) -d.d. by induction, and since q is also (j, y) -d.d. by (iii), we also have the required factorization in this case. \square

3. APPLYING THE HEATH-BROWN IDENTITY

The goal of this and the next sections is to prove the assumption $\text{MPZ}^{(i)}[\varpi, \delta]$ (Definition 2.3) for as wide a range of ϖ and δ as possible, following the outline in Section 1.1. The first step, which we implement in this section, is the proof of Lemma 2.7. We follow standard arguments, particularly those in [52]. The main tool is the Heath-Brown identity, which is combined with a purely combinatorial result about finite sets of non-negative numbers. We begin with the latter statement:

Lemma 3.1. *Let $1/10 < \sigma < 1/2$, and let t_1, \dots, t_n be non-negative real numbers such that $t_1 + \dots + t_n = 1$. Then at least one of the following three statements holds:*

(Type 0) *There is a t_i with $t_i \geq 1/2 + \sigma$.*

(Type I/II) *There is a partition $\{1, \dots, n\} = S \cup T$ such that*

$$\frac{1}{2} - \sigma < \sum_{i \in S} t_i \leq \sum_{i \in T} t_i < \frac{1}{2} + \sigma.$$

(Type III) *There exist distinct i, j, k with $2\sigma \leq t_i \leq t_j \leq t_k \leq 1/2 - \sigma$ and*

$$t_i + t_j, t_i + t_k, t_j + t_k \geq \frac{1}{2} + \sigma. \quad (3.1)$$

Furthermore, if $\sigma > 1/6$, then the Type III alternative cannot occur.

Proof. We dispose of the final claim first: if $\sigma > 1/6$, then $2\sigma > 1/2 - \sigma$, and so the inequalities $2\sigma \leq t_i \leq t_j \leq t_k \leq 1/2 - \sigma$ of the Type III alternative are inconsistent.

Now we prove the main claim. Let σ and (t_1, \dots, t_n) be as in the statement. We assume that the Type 0 and Type I/II statements are false, and will deduce that the Type III statement holds.

From the failure of the Type 0 conclusion, we know that

$$t_i < \frac{1}{2} + \sigma \quad (3.2)$$

for all $i = 1, \dots, n$. From the failure of the Type I/II conclusion, we also know that, for any $S \subset \{1, \dots, n\}$, we have

$$\sum_{i \in S} t_i \notin \left(\frac{1}{2} - \sigma, \frac{1}{2} + \sigma \right)$$

since otherwise we would obtain the conclusion of Type I/II by taking T to be the complement of S , possibly after swapping the role of S and T .

We say that a set $S \subset \{1, \dots, n\}$ is *large* if $\sum_{i \in S} t_i \geq \frac{1}{2} + \sigma$, and that it is *small* if $\sum_{i \in S} t_i \leq \frac{1}{2} - \sigma$. Thus, the previous observation shows that every set $S \subset \{1, \dots, n\}$ is either large or small, and also (from (3.2)) that singletons are small, as is the empty set. Also, it is immediate that the complement of a large set is small, and conversely (since $t_1 + \dots + t_n = 1$).

Further, we say that an element $i \in \{1, \dots, n\}$ is *powerful* if there exists a small set $S \subset \{1, \dots, n\} \setminus \{i\}$ such that $S \cup \{i\}$ is large, i.e., if i can be used to turn a small set into a large set. Then we say that an element i is *powerless* if it is not powerful. Thus, adding or removing a powerless element from a set S cannot alter its smallness or largeness, and in particular, the union of a small set and a set of powerless elements is small.

We claim that there exist exactly three powerful elements. First, there must be at least two, because if P is the set of powerless elements, then it is small, and hence its complement is large, and thus contains at least two elements, which are powerful. But picking one of these powerful i , the set $\{i\} \cup P$ is small, and therefore its complement also has at least two elements, which together with i are three powerful elements.

Now, we observe that if i is powerful, then $t_i \geq 2\sigma$, since the gap between a large sum $\sum_{j \in S \cup \{i\}} t_j$ and a small sum $\sum_{j \in S} t_j$ is at least 2σ . In particular, if $i \neq j$ are two powerful numbers, then

$$t_i + t_j \geq 4\sigma > \frac{1}{2} - \sigma,$$

where the second inequality holds because of the assumption $\sigma > 1/10$. Thus the set $\{i, j\}$ is not small, and is therefore large. But then if $\{i, j, k, l\}$ was a set of four powerful elements, it would follow that

$$1 = t_1 + \cdots + t_n \geq (t_i + t_j) + (t_k + t_l) \geq 2\left(\frac{1}{2} + \sigma\right) > 1,$$

a contradiction.

Let therefore i, j, k be the three powerful elements. We may order them so that $t_i \leq t_j \leq t_k$. We have

$$2\sigma \leq t_i \leq t_j \leq t_k \leq \frac{1}{2} - \sigma$$

by (3.2) and the previous argument, which also shows that $\{i, j\}$, $\{i, k\}$ and $\{j, k\}$ are large, which is (3.1). \square

Remark 3.2. For $1/10 < \sigma \leq 1/6$, the Type III case can indeed occur, as can be seen by considering the examples $(t_1, t_2, t_3) = (2\sigma, 1/2 - \sigma, 1/2 - \sigma)$. The lemma may be extended to the range $1/14 < \sigma < 1/2$, but at the cost of adding two additional cases (corresponding to the case of four or five powerful elements respectively):

(Type IV) There exist distinct i, j, k, l with $2\sigma \leq t_i \leq t_j \leq t_k \leq t_l \leq 1/2 - \sigma$ and $t_i + t_l \geq 1/2 + \sigma$.

(Type V) There exist distinct i, j, k, l, m with $2\sigma \leq t_i \leq t_j \leq t_k \leq t_l \leq t_m \leq 1/2 - \sigma$ and $t_i + t_j + t_k \geq 1/2 + \sigma$.

We leave the verification of this extension to the reader. Again, for $1/14 < \sigma \leq 1/10$, the Type IV and Type V cases can indeed occur, as can be seen by considering the examples $(t_1, t_2, t_3, t_4) = (2\sigma, 2\sigma, 1/2 - 3\sigma, 1/2 - \sigma)$ and $(t_1, t_2, t_3, t_4, t_5) = (2\sigma, 2\sigma, 2\sigma, 2\sigma, 1 - 8\sigma)$. With this extension, it is possible to extend Lemma 2.7 to the regime $1/14 < \sigma < 1/2$, but at the cost of requiring additional “Type IV” and “Type V” estimates as hypotheses. Unfortunately, while the methods in this paper do seem to be able to establish some Type IV estimates, they do not seem to give enough Type V estimates to make it profitable to try to take σ below $1/10$.

To apply Lemma 3.1 to distribution theorems concerning the von Mangoldt function Λ , we recall the Heath-Brown identity (see [26] or [30, Prop. 13.3]).

Lemma 3.3 (Heath-Brown identity). *For any $K \geq 1$, we have the identity*

$$\Lambda = \sum_{j=1}^K (-1)^{j-1} \binom{K}{j} \mu_{\leq}^{*j} \star \mathbf{1}^{*(j-1)} \star L \quad (3.3)$$

on the interval $[x, 2x]$, where $\mathbf{1}$ is the constant function $\mathbf{1}(n) := 1$, L is the logarithm function $L(n) := \log n$, μ_{\leq} is the truncated Möbius function

$$\mu_{\leq}(n) := \mu(n) \mathbf{1}_{n \leq (2x)^{1/K}},$$

and where we denote $f^{*j} = f \star \cdots \star f$ the j -fold Dirichlet convolution of an arithmetic function f , i.e.,

$$f^{*j}(n) := \sum_{a_1 \cdots a_j = n} f(a_1) \cdots f(a_j).$$

Proof. Write $\mu = \mu_{\leq} + \mu_{>}$, where $\mu_{>}(n) := \mu(n)\mathbf{1}_{n > (2x)^{1/K}}$. Clearly the convolution

$$\mu_{>}^{\star K} \star \mathbf{1}^{\star(K-1)} \star L$$

vanishes on $[1, 2x]$. Expanding out $\mu_{>} = \mu - \mu_{\leq}$ and using the binomial formula, we conclude that

$$0 = \sum_{j=0}^K (-1)^j \binom{K}{j} \mu^{\star(K-j)} \star \mu_{\leq}^{\star j} \star \mathbf{1}^{\star(K-1)} \star L \quad (3.4)$$

on $[x, 2x]$. Since Dirichlet convolution is associative, the standard identities $\Lambda = \mu \star L$ and $\delta = \mu \star \mathbf{1}$ (where the Kronecker delta function $\delta(n) := \mathbf{1}_{n=1}$ is the unit for Dirichlet convolution) show that the $j = 0$ term of (3.4) is

$$\mu^{\star K} \star \mathbf{1}^{\star(K-1)} \star L = \mu \star L = \Lambda.$$

For all the other terms, we can use commutativity of Dirichlet convolution and (again) $\mu \star \mathbf{1} = \delta$ to write

$$\mu^{\star(K-j)} \star \mu_{\leq}^{\star j} \star \mathbf{1}^{\star(K-1)} \star L = \mu_{\leq}^{\star j} \star \mathbf{1}^{\star(j-1)} \star L,$$

so that we get (3.3). \square

We will now prove Lemma 2.7, which the reader is invited to review. Let $i, \varpi, \delta, \sigma$ satisfy the hypotheses of that lemma, and let $A_0 > 0$ be fixed. By the definition of $\text{MPZ}^{(i)}(\varpi, \delta)$, which is the conclusion of the lemma, it suffices to show that for any $Q \ll x^{1/2+2\varpi}$, any bounded set $I \subset (0, \infty)$ and any residue class $a \pmod{P_I}$, we have

$$\sum_{q \in \mathcal{Q}} |\Delta(\Lambda \mathbf{1}_{[x, 2x]}; a \pmod{q})| \ll x \log^{-A_0+O(1)} x, \quad (3.5)$$

where

$$\mathcal{Q} := \{q \leq Q : q \in \mathcal{D}_I^{(i)}(x^\delta)\} \quad (3.6)$$

(recalling the definition (2.2)) and the $O(1)$ term in the exponent is independent of A_0 .

Let K be any fixed integer with

$$\frac{1}{K} < 2\sigma \quad (3.7)$$

(e.g. one can take $K = 10$). We apply Lemma 3.3 with this value of K . By the triangle inequality, it suffices to show that

$$\sum_{q \in \mathcal{Q}} |\Delta((\mu_{\leq}^{\star j} \star \mathbf{1}^{\star(j-1)} \star L) \mathbf{1}_{[x, 2x]}; a \pmod{q})| \ll x \log^{-A_0/2+O(1)} x \quad (3.8)$$

for each $1 \leq j \leq K$, which we now fix.

The next step is a finer-than-dyadic decomposition (a standard idea going back at least to Fouvry [10] and Fouvry-Iwaniec [13]). We denote $\Theta := 1 + \log^{-A_0} x$. Let $\psi: \mathbb{R} \rightarrow \mathbb{R}$ be a smooth function supported on $[-\Theta, \Theta]$ that is equal to 1 on $[-1, 1]$ and obeys the derivative estimates

$$|\psi^{(m)}(x)| \ll \log^{mA_0} x$$

for $x \in \mathbb{R}$ and any fixed $m \geq 0$, where the implied constant depends only on m . We then have a smooth partition of unity

$$1 = \sum_{N \in \mathcal{D}} \psi_N(n)$$

indexed by the multiplicative semigroup

$$\mathcal{D} := \{\Theta^m : m \in \mathbb{N} \cup \{0\}\}$$

for any natural number n , where

$$\psi_N(n) := \psi\left(\frac{n}{N}\right) - \psi\left(\frac{\Theta n}{N}\right)$$

is supported in $[\Theta^{-1}N, \Theta N]$. We thus have decompositions

$$1 = \sum_{N \in \mathcal{D}} \psi_N, \quad \mu_{\leq} = \sum_{N \in \mathcal{D}} \psi_N \mu_{\leq}, \quad L = \sum_{N \in \mathcal{D}} \psi_N L.$$

For $1 \leq j \leq K$, we have

$$\begin{aligned} (\mu_{\leq}^{\star j} \star 1^{\star(j-1)} \star L) \mathbf{1}_{[x, 2x]} &= \sum_{N_1, \dots, N_{2j} \in \mathcal{D}} \{(\psi_{N_1} \mu_{\leq}) \star \dots \star (\psi_{N_j} \mu_{\leq}) \\ &\quad \star \psi_{N_{j+1}} \star \dots \star \psi_{N_{2j-1}} \star \psi_{N_{2j}} L\} \mathbf{1}_{[x, 2x]} \\ &= \sum_{N_1, \dots, N_{2j} \in \mathcal{D}} \log(N_{2j}) \{(\psi_{N_1} \mu_{\leq}) \star \dots \star (\psi_{N_j} \mu_{\leq}) \\ &\quad \star \psi_{N_{j+1}} \star \dots \star \psi_{N_{2j-1}} \star \psi'_{N_{2j}}\} \mathbf{1}_{[x, 2x]} \end{aligned}$$

where $\psi'_N := \psi_N \frac{L}{\log N}$ is a simple variant of ψ_N .

For each N_1, \dots, N_{2j} , the summand in this formula vanishes unless

$$N_1, \dots, N_j \ll x^{1/K} \quad (3.9)$$

and

$$\frac{x}{\Theta^{2K}} \leq N_1 \dots N_{2j} \leq 2x \Theta^{2K}.$$

In particular, it vanishes unless

$$x \left(1 - O\left(\frac{1}{\log^{A_0} x}\right)\right) \leq N_1 \dots N_{2j} \leq 2x \left(1 + O\left(\frac{1}{\log^{A_0} x}\right)\right). \quad (3.10)$$

We conclude that there are at most

$$\ll \log^{2j(A_0+1)} x \quad (3.11)$$

tuples $(N_1, \dots, N_{2j}) \in \mathcal{D}^{2j}$ for which the summand is non-zero. Let \mathcal{E} be the set of these tuples. We then consider the arithmetic function

$$\begin{aligned} \alpha &= \sum_{(N_1, \dots, N_{2j}) \in \mathcal{E}} \log(N_{2j}) \{(\psi_{N_1} \mu_{\leq}) \star \dots \star (\psi_{N_j} \mu_{\leq}) \star \psi_{N_{j+1}} \star \dots \star \psi_{N_{2j-1}} \star \psi'_{N_{2j}}\} \\ &\quad - (\mu_{\leq}^{\star j} \star 1^{\star j-1} \star L) \mathbf{1}_{[x, 2x]}. \end{aligned} \quad (3.12)$$

Note that the cutoff $\mathbf{1}_{[x, 2x]}$ is only placed on the second term in the definition of α , and is not present in the first term.

By the previous remarks, this arithmetic function is supported on

$$[x(1 - O(\log^{-A_0} x)), x] \cup [2x, 2x(1 + O(\log^{-A_0} x))]$$

and using the divisor bound and trivial estimates, it satisfies

$$\alpha(n) \ll \tau(n)^{O(1)} (\log n)^{O(1)},$$

where the exponents are bounded independently of A_0 . In particular, we deduce from Lemma 1.3 that

$$\Delta(\alpha; a(q)) \ll x \log^{-A_0+O(1)} x$$

for all $q \geq 1$. Using the estimate (3.11) for the number of summands in \mathcal{E} , we see that, in order to prove (3.8), it suffices to show that

$$\sum_{q \in \mathcal{Q}} |\Delta(\alpha_1 \star \cdots \star \alpha_{2j}; a(q))| \ll x \log^{-A} x \quad (3.13)$$

for $A > 0$ arbitrary, where each α_i is an arithmetic function of the form $\psi_{N_i} \mu_{\leq}$, ψ_{N_i} or ψ'_{N_i} , where (N_1, \dots, N_{2j}) satisfy (3.9) and (3.10).

We now establish some basic properties of the arithmetic functions α_k that may occur. For a subset $S \subset \{1, \dots, 2j\}$, we will denote by

$$\alpha_S := \star_{k \in S} \alpha_k$$

the convolution of the α_k for $k \in S$.

Lemma 3.4. *Let $1 \leq k \leq 2j$ and $S \subset \{1, \dots, 2j\}$. The following facts hold:*

- (i) *Each α_k is a coefficient sequence located at scale N_k , and more generally, the convolution α_S is a coefficient sequence located at scale $\prod_{k \in S} N_k$.*
- (ii) *If $N_k \gg x^{2\sigma}$, then α_k is smooth at scale N_k .*
- (iii) *If $N_k \gg x^\varepsilon$ for some fixed $\varepsilon > 0$, then α_k satisfies the Siegel-Walfisz property. More generally, α_S satisfies the Siegel-Walfisz property if $\prod_{k \in S} N_k \gg x^\varepsilon$ for some fixed $\varepsilon > 0$.*
- (iv) $N_1 \dots N_{2j} \asymp x$.

Proof. The first part of (i) is clear from construction. For the second part of (i), we use the easily verified fact that if α, β are coefficient sequences located at scales N, M respectively, then $\alpha \star \beta$ is a coefficient sequence located at scale NM .

For (ii), we observe that since $2\sigma > K^{-1}$, the condition $N_k \gg x^{2\sigma}$ can only occur for $k > j$ in view of (3.9), so that α_k takes the form ψ_{N_k} or ψ'_{N_k} , and the smoothness then follows directly from the definitions.

For (iii), the Siegel-Walfisz property for α_k when $k \leq j$ follows from the Siegel-Walfisz theorem for the Möbius function and for Dirichlet characters (see e.g. [49, Satz 4] or [30, Th. 5.29]), using summation by parts to handle the smooth cutoff, and we omit the details. For $k > j$, α_k is smooth, and the Siegel-Walfisz property for α_k follows from the Poisson summation formula (and the rapid decay of the Fourier transform of smooth, compactly supported functions; compare with the arguments at the end of this section for the Type 0 case).

To handle the general case, it therefore suffices to check that if α, β are coefficient sequences located at scales N, M respectively with $x^\varepsilon \ll M \ll x^C$ for some fixed $\varepsilon, C > 0$, and β satisfies the Siegel-Walfisz property, then so does $\alpha \star \beta$. This is again relatively standard, but we give the proof for completeness.

By Definition 2.5, our task is to show that

$$|\Delta((\alpha \star \beta) \mathbf{1}_{(\cdot, q)=1}; a(r))| \ll \tau(qr)^{O(1)} N \log^{-A} x$$

for any $q, r \geq 1$, any fixed A , and any primitive residue class $a(r)$. We replace α, β by their restriction to integers coprime to qr (without indicating this in the notation), which allows us to remove the constraint $\mathbf{1}_{(n, q)=1}$. We may also assume that $r = O(\log^{A+O(1)} x)$,

since the desired estimate follows from the trivial estimate (2.7) for the discrepancy otherwise.

For any integer n , we have

$$\sum_{n=a \pmod{r}} (\alpha \star \beta)(n) = \sum_{b \in (\mathbb{Z}/r\mathbb{Z})^\times} \left(\sum_{d=b \pmod{r}} \alpha(d) \right) \left(\sum_{m=\bar{b}a \pmod{r}} \beta(m) \right)$$

and

$$\begin{aligned} \sum_n (\alpha \star \beta)(n) &= \left(\sum_d \alpha(d) \right) \left(\sum_m \beta(m) \right) \\ &= \sum_{b \in (\mathbb{Z}/r\mathbb{Z})^\times} \left(\sum_{d=b \pmod{r}} \alpha(d) \right) \left(\sum_m \beta(m) \right) \end{aligned}$$

so that

$$|\Delta(\alpha \star \beta, a \pmod{r})| \leq \sum_{b \in (\mathbb{Z}/r\mathbb{Z})^\times} \left| \sum_{d=b \pmod{r}} \alpha(d) \right| |\Delta(\beta; \bar{b}a \pmod{r})|.$$

From (1.4) (and Definition (2.5)), we have

$$\sum_{d=b \pmod{r}} \alpha(d) \ll \frac{N}{r} \tau(r)^{O(1)} \log^{O(1)} x + N^{o(1)}$$

for any $b \pmod{r}$, and since β has the Siegel-Walfisz property, we have

$$|\Delta(\beta; \bar{b}a \pmod{r})| \ll \tau(r)^{O(1)} M \log^{-B} x$$

for any $b \pmod{r}$ and any fixed $B > 0$. Thus

$$\begin{aligned} |\Delta(\alpha \star \beta, a \pmod{r})| &\ll \tau(r)^{O(1)} \varphi(r) \left(\frac{N}{r} + N^{o(1)} \right) M \log^{-B+O(1)} x \\ &\ll \tau(r)^{O(1)} M N \log^{-B+O(1)} x \end{aligned}$$

by the assumption concerning the size of r .

Finally, the claim (iv) follows from (3.10). \square

We can now conclude this section by showing how the assumptions $\text{Type}_I^{(i)}[\varpi, \delta, \sigma]$, $\text{Type}_{II}^{(i)}[\varpi, \delta]$ and $\text{Type}_{III}^{(i)}[\varpi, \delta, \sigma]$ of Lemma 2.7 imply the estimates (3.13).

Let therefore $(\alpha_1, \dots, \alpha_{2j})$ be given with the condition of (3.13). By Lemma 3.4(iv), we can write $N_k \asymp x^{t_k}$ for $k = 1, \dots, 2j$, where the t_k are non-negative reals (not necessarily fixed) that sum to 1. By Lemma 3.1, the t_i satisfy one of the three conclusions (Type 0), (Type I/II), (Type III) of that lemma. We deal with each in turn. The first case can be dealt with directly, while the others require one of the assumptions of Lemma 2.7, and we begin with these.

Suppose that we are in the Type I/II case, with the partition $\{1, \dots, 2j\} = S \cup T$ given by the combinatorial lemma. We have

$$\alpha_1 \star \dots \star \alpha_{2j} = \alpha_S \star \alpha_T.$$

By Lemma 3.4, α_S, α_T are coefficient sequences located at scales N_S, N_T respectively, where

$$N_S N_T \asymp x,$$

and (by (iii)) α_S and α_T satisfy the Siegel-Walfisz property. By Lemma 3.1, we also have

$$x^{1/2-\sigma} \ll N_S \ll N_T \ll x^{1/2+\sigma}.$$

Thus, directly from Definition 2.6 and (3.6), the required estimate (3.13) follows either from the hypothesis $\text{Type}_I^{(i)}[\varpi, \delta, \sigma]$ (if one has $N_S \leq x^{1/2-2\varpi-c}$ for some sufficiently small fixed $c > 0$) or from $\text{Type}_{II}^{(i)}[\varpi, \delta]$ (if $N_S > x^{1/2-2\varpi-c}$, for the same value of c).

Similarly, in the Type III case, comparing Lemmas 3.4 and 3.1 with Definition 2.6 and (3.6) shows that (3.8) is a direct translation of $\text{Type}_{III}^{(i)}[\varpi, \delta, \sigma]$.

It remains to prove (3.8) in the Type 0 case, and we can do this directly. In this case, there exists some $k \in \{1, \dots, 2j\}$, such that $t_k \geq 1/2 + \sigma > 2\sigma$. Intuitively, this means that α_k is smooth (by Lemma 3.4 (ii)) and has a long support, so that it is very well-distributed in arithmetic progressions to relatively large moduli, and we can just treat the remaining α_j trivially.

Precisely, we write

$$\alpha_1 \star \dots \star \alpha_{2j} = \alpha_k \star \alpha_S$$

where $S = \{1, \dots, 2j\} \setminus \{k\}$. By Lemma 3.4, α_k is a coefficient sequence which is smooth at a scale $N_k \gg x^{1/2+\sigma}$, and α_S is a coefficient sequence which is located at a scale N_S with $N_k N_S \asymp x$. We argue as in Lemma 3.4(iii): we have

$$\Delta(\alpha_k \star \alpha_S; a(q)) = \sum_{m \in (\mathbb{Z}/q\mathbb{Z})^\times} \sum_{\ell=m} \alpha_S(\ell) \Delta(\alpha_k; \bar{m}a(q))$$

and since

$$\sum_m |\alpha_S(m)| \ll N_S,$$

(by (1.3) and Definition 2.5), we get

$$\sum_{q \in \mathcal{Q}} |\Delta(\alpha_1 \star \dots \star \alpha_{2j}; a(q))| \ll N_S \sum_{q \leq Q} \sup_{b \in (\mathbb{Z}/q\mathbb{Z})^\times} |\Delta(\alpha_k; b(q))|. \quad (3.14)$$

Since α_k is smooth at scale N_k , we can write

$$\alpha_k(n) = \psi(n/N_k)$$

for some smooth function $\psi: \mathbb{R} \rightarrow \mathbb{R}$ supported on an interval of size $\ll 1$, which satisfies the estimates

$$|\psi^{(j)}(t)| \ll 1$$

for all t and all fixed $j \geq 0$. By the Poisson summation formula, we have

$$\sum_{n=b(q)} \alpha_k(n) = \frac{N_k}{q} \sum_{m \in \mathbb{Z}} e_q(mb) \hat{\psi}\left(\frac{mN_k}{q}\right) = \frac{N_k}{q} \hat{\psi}(0) + \frac{N_k}{q} \sum_{m \neq 0} e_q(mb) \hat{\psi}\left(\frac{mN_k}{q}\right),$$

for $q \geq 1$ and $b(q)$, where

$$\hat{\psi}(s) := \int_{\mathbb{R}} \psi(t) e(-ts) dt$$

is the Fourier transform of ψ . From the smoothness and support of ψ , we get the bound

$$\left| \hat{\psi}\left(\frac{mN_k}{q}\right) \right| \ll \left(\frac{mN_k}{q} \right)^{-2}$$

for $m \neq 0$ and $q \leq Q$, and thus we derive

$$\sum_{n=b \pmod{q}} \alpha_k(n) = \frac{N_k}{q} \hat{\psi}(0) + O\left(\frac{N_k}{q} (N_k/q)^{-2}\right).$$

Since by definition

$$|\Delta(\alpha_k; b \pmod{q})| = \sum_{n=b \pmod{q}} \alpha_k(n) - \frac{1}{\varphi(q)} \sum_{c \in (\mathbb{Z}/q\mathbb{Z})^\times} \sum_{n=c \pmod{q}} \alpha_k(n),$$

we get

$$|\Delta(\alpha_k; b \pmod{q})| \ll \frac{N_k}{q} (N_k/q)^{-2}.$$

Therefore, from (3.14), we have

$$\sum_{q \in \mathcal{Q}} |\Delta(\alpha_1 \star \cdots \star \alpha_{2j}; a \pmod{q})| \ll N_S N_k \left(\frac{Q}{N_k}\right)^2 \ll x^{1-2\sigma+4\varpi},$$

and since $\sigma > 2\varpi$ (by assumption in Lemma 2.7), this implies (3.13), which concludes the proof of Lemma 2.7.

Remark 3.5. In the case $\sigma > 1/6$, one can replace the Heath-Brown identity of Lemma 3.3 with other decompositions of the von Mangoldt function Λ , and in particular with the well-known *Vaughan identity*

$$\Lambda_{\geq} = \mu_{<} \star L - \mu_{<} \star \Lambda_{<} \star 1 + \mu_{\geq} \star \Lambda_{\geq} \star 1$$

from [50], where

$$\Lambda_{\geq}(n) := \Lambda(n) \mathbf{1}_{n \geq V}, \quad \Lambda_{<}(n) := \Lambda(n) \mathbf{1}_{n < V} \quad (3.15)$$

$$\mu_{\geq}(n) := \mu(n) \mathbf{1}_{n \geq U}, \quad \mu_{<}(n) := \mu(n) \mathbf{1}_{n < U}, \quad (3.16)$$

where $U, V > 1$ are arbitrary parameters. Setting $U = V = x^{1/3}$, we then see that to show (3.5), it suffices to establish the bounds

$$\sum_{q \in \mathcal{Q}} |\Delta((\mu_{<} \star L) \mathbf{1}_{[x, 2x]}; a \pmod{q})| \ll x \log^{-A_0/2+O(1)} x \quad (3.17)$$

$$\sum_{q \in \mathcal{Q}} |\Delta((\mu_{<} \star \Lambda_{<} \star 1) \mathbf{1}_{[x, 2x]}; a \pmod{q})| \ll x \log^{-A_0/2+O(1)} x \quad (3.18)$$

$$\sum_{q \in \mathcal{Q}} |\Delta((\mu_{\geq} \star \Lambda_{\geq} \star 1) \mathbf{1}_{[x, 2x]}; a \pmod{q})| \ll x \log^{-A_0/2+O(1)} x. \quad (3.19)$$

To prove (3.17), we may perform dyadic decomposition on $\mu_{<}$ and L , much as in the previous arguments. The components of L which give a non-trivial contribution to (3.17) will be located at scales $\gg x^{2/3}$. One can then use the results of the Type 0 analysis above. In order to prove (3.19), we similarly decompose the $\mu_{\geq}, \Lambda_{\geq}$, and 1 factors and observe that the resulting components of μ_{\geq} and $\Lambda_{\geq} \star 1$ that give a non-trivial contribution to (3.19) will be located at scales M, N with $x^{1/3} \ll M, N \ll x^{2/3}$ and $MN \asymp x$, and one can then argue using Type I and Type II estimates as before since $\sigma > 1/6$. Finally, for (3.18), we decompose $\mu_{<} \star \Lambda_{<}$, and 1 into components at scales M, N respectively with $M \ll x^{2/3}$ and $MN \asymp x$, so $N \gg x^{1/3}$. If $N \gg x^{2/3}$, then the Type 0 analysis applies again, and otherwise we may use the Type I and Type II estimates with $\sigma > 1/6$.

Remark 3.6. An inspection of the arguments shows that the interval $[x, 2x]$ used in Lemma 2.7 may be replaced by a more general interval $[x_1, x_2]$ for any $x \leq x_1 \leq x_2 \leq 2x$, leading to a slight generalization of the conclusion $\text{MPZ}^{(i)}[\varpi, \delta]$. By telescoping series, one may then generalize the intervals $[x_1, x_2]$ further, to the range $1 \leq x_1 \leq x_2 \leq 2x$.

In the next sections, we will turn our attention to the task of proving distribution estimates of Type I, II and III. All three turn out to be intimately related to estimates for exponential sums over $\mathbb{Z}/q\mathbb{Z}$, either “complete” sums over all of $\mathbb{Z}/q\mathbb{Z}$ or “incomplete” sums over suitable subsets, such as reductions modulo q of intervals or arithmetic progressions (this link goes back to the earliest works in proving distribution estimates beyond the range of the large sieve). In the next section, we consider the basic theory of the simplest of those sums, where the essential results go back to Weil’s theory of exponential sums in one variable over finite fields. These are enough to handle basic Type I and II estimates, which we consider next. On the other hand, for Type III estimates and the most refined Type I estimates, we require the much deeper results and insights of Deligne’s second proof of the Riemann Hypothesis for algebraic varieties over finite fields.

4. ONE-DIMENSIONAL EXPONENTIAL SUMS

The results of this section are very general and are applicable to many problems in analytic number theory. Since the account we provide might well be useful as a general reference beyond the applications to the main results of this paper, we will not use the asymptotic convention of Definition 1.2, but provide explicit estimates that can easily be quoted in other contexts. (In particular, we will sometimes introduce variables named x in our notation.)

4.1. Preliminaries. We begin by setting up some notation and conventions. We recall from Section 1.3 that we defined $e_q(a) = e^{2\pi i a/q}$ for $a \in \mathbb{Z}$ and $q \geq 1$. This is a group homomorphism $\mathbb{Z} \rightarrow \mathbb{C}^\times$, and since $q\mathbb{Z} \subset \ker e_q$, it induces naturally a homomorphism, which we also denote e_q , from $\mathbb{Z}/q\mathbb{Z}$ to \mathbb{C}^\times . In fact, for any multiple qr of q , we can also view e_q as a homomorphism $\mathbb{Z}/qr\mathbb{Z} \rightarrow \mathbb{C}^\times$.

It is convenient for us (and compatible with the more algebraic theory for multi-variable exponential sums discussed in Section 6) to extend further e_q to the projective line $\mathbb{P}^1(\mathbb{Z}/q\mathbb{Z})$ by extending it by zero to the point(s) at infinity. Precisely, recall that $\mathbb{P}^1(\mathbb{Z}/q\mathbb{Z})$ is the quotient of

$$X_q = \{(a, b) \in (\mathbb{Z}/q\mathbb{Z})^2 : a \text{ and } b \text{ have no common factor}\},$$

(where a common factor of a and b is a prime $p \mid q$ such that a and b are zero modulo p) by the equivalence relation

$$(a, b) = (ax, bx)$$

for all $x \in (\mathbb{Z}/q\mathbb{Z})^\times$. We identify $\mathbb{Z}/q\mathbb{Z}$ with a subset of $\mathbb{P}^1(\mathbb{Z}/q\mathbb{Z})$ by sending x to the class of $(x, 1)$. We note that

$$|\mathbb{P}^1(\mathbb{Z}/q\mathbb{Z})| = q \prod_{p|q} \left(1 + \frac{1}{p}\right),$$

and that a point $(a, b) \in \mathbb{P}^1(\mathbb{Z}/q\mathbb{Z})$ belongs to $\mathbb{Z}/q\mathbb{Z}$ if and only if $b \in (\mathbb{Z}/q\mathbb{Z})^\times$, in which case $(a, b) = (ab^{-1}, 1)$.

Thus, we can extend e_q to $\mathbb{P}^1(\mathbb{Z}/q\mathbb{Z})$ by defining

$$e_q((a, b)) = e_q(ab^{-1})$$

if $b \in (\mathbb{Z}/q\mathbb{Z})^\times$, and $e_q((a, b)) = 0$ otherwise.

We have well-defined reduction maps $\mathbb{P}^1(\mathbb{Z}/qr\mathbb{Z}) \rightarrow \mathbb{P}^1(\mathbb{Z}/q\mathbb{Z})$ for all integers $r \geq 1$, as well as $\mathbb{P}^1(\mathbb{Q}) \rightarrow \mathbb{P}^1(\mathbb{Z}/q\mathbb{Z})$, and we can therefore also naturally define $e_q(x)$ for $x \in \mathbb{P}^1(\mathbb{Z}/qr\mathbb{Z})$ or for $x \in \mathbb{P}^1(\mathbb{Q})$ (for the map $\mathbb{P}^1(\mathbb{Q}) \rightarrow \mathbb{P}^1(\mathbb{Z}/q\mathbb{Z})$, we use the fact that any $x \in \mathbb{P}^1(\mathbb{Q})$ is the class of (a, b) where a and b are coprime integers, so that $(a(q), b(q)) \in X_q$).

We will use these extensions especially in the following context: let $P, Q \in \mathbb{Z}[X]$ be polynomials, with Q non-zero, and consider the rational function $f = \frac{P}{Q} \in \mathbb{Q}(X)$. This defines a map $\mathbb{P}^1(\mathbb{Q}) \rightarrow \mathbb{P}^1(\mathbb{Q})$, and then by reduction modulo q , a map

$$f(q): \mathbb{P}^1(\mathbb{Z}/q\mathbb{Z}) \rightarrow \mathbb{P}^1(\mathbb{Z}/q\mathbb{Z}).$$

We can therefore consider the function $x \mapsto e_q(f(x))$ for $x \in \mathbb{Z}/q\mathbb{Z}$. If $x \in \mathbb{Z}$ is such that $Q(x)$ is coprime to q , then this is just $e_q(P(x)\overline{Q(x)})$. If $Q(x)$ is not coprime to q , on the other hand, one must be a bit careful. If q is prime, then one should write $f(q) = P_1/Q_1$ with $P_1, Q_1 \in (\mathbb{Z}/q\mathbb{Z})[X]$ coprime, and then $e_q(f(x)) = e_q(P_1(x)\overline{Q_1(x)})$ if $Q_1(x) \neq 0$, while $e_q(f(x)) = 0$ otherwise. If q is squarefree, one combines the prime components according to the Chinese Remainder Theorem, as we will recall later.

Example 4.1. Let $P = X$, $Q = X + 3$ and $q = 3$, and set $f := \frac{P}{Q}$. Then, although $P(q)$ and $Q(q)$ both take the value 0 at $x = 0 \in \mathbb{Z}/q\mathbb{Z}$, we have $e_q(f(0)) = 1$.

In rare cases (in particular the proof of Proposition 8.4 in Section 8.4) we will use one more convention: quantities

$$e_p\left(\frac{a}{b}\right)$$

may arise where a and b are integers that depend on other parameters, and with b allowed to be divisible by p . However, this will only happen when the formula is to be interpreted as

$$e_p\left(\frac{a}{b}\right) = \psi\left(\frac{1}{b}\right) = \psi(\infty)$$

where $\psi(x) = e_p(ax)$ defines an additive character of \mathbb{F}_p . Thus we use the convention

$$e_p\left(\frac{a}{b}\right) = \begin{cases} 0 & \text{if } a \not\equiv 0 \pmod{p}, b \equiv 0 \pmod{p} \\ 1 & \text{if } a \equiv 0 \pmod{p}, b \equiv 0 \pmod{p}, \end{cases}$$

since in the second case, we are evaluating the trivial character at ∞ .

4.2. Complete exponential sums over a finite field. As is well known since early works of Davenport and Hasse in particular, the Riemann Hypothesis for curves over finite fields (proven by Weil [51]) implies bounds with “square root cancellation” for one-dimensional exponential sums over finite fields. A special case is the following general bound:

Lemma 4.2 (One-variable exponential sums with additive characters). *Let $P, Q \in \mathbb{Z}[X]$ be polynomials over \mathbb{Z} in one indeterminate X . Let p be a prime number such that $Q(p) \in \mathbb{F}_p[X]$ is non-zero, such that there is no identity of the form*

$$\frac{P}{Q}(p) = g^p - g + c \tag{4.1}$$

in $\mathbb{F}_p(X)$ for some rational function $g = g(X) \in \mathbb{F}_p(X)$ and some $c \in \mathbb{F}_p$. Then we have

$$\left| \sum_{x \in \mathbb{F}_p} e_p \left(\frac{P(x)}{Q(x)} \right) \right| \ll \sqrt{p} \quad (4.2)$$

where the implicit constant depends only on $\max(\deg P, \deg Q)$, and this dependency is linear.

Note that, by our definitions, we have

$$\sum_{x \in \mathbb{F}_p} e_p \left(\frac{P(x)}{Q(x)} \right) = \sum_{\substack{x \in \mathbb{F}_p \\ Q_1(x) \neq 0}} e_p(P_1(x) \overline{Q_1(x)}),$$

where $P/Q(p) = P_1/Q_1$ with $P_1, Q_1 \in \mathbb{F}_p[X]$ coprime polynomials.

As key examples of Lemma 4.2, we record Weil's bound for Kloosterman sums, namely

$$\left| \sum_{x \in \mathbb{F}_p} e_p \left(ax + \frac{b}{x} \right) \right| \ll \sqrt{p} \quad (4.3)$$

when $a, b \in \mathbb{F}_p$ are not both zero, as well as the variant

$$\left| \sum_{x \in \mathbb{F}_p} e_p \left(ax + \frac{b}{x} + \frac{c}{x+l} + \frac{d}{x+m} + \frac{e}{x+l+m} \right) \right| \ll \sqrt{p} \quad (4.4)$$

for $a, b, c, d, e, l, m \in \mathbb{F}_p$ with $b, c, d, e, l, m, l+m$ non-zero. In fact, these two estimates are almost the only two cases of Lemma 4.2 that are needed in our arguments. In both cases, one can determine a suitable implied constant, e.g., the Kloosterman sum in (4.3) has modulus at most $2\sqrt{p}$.

We note also that the case (4.1) must be excluded, since $g^p(x) - g(x) + c = c$ for all $x \in \mathbb{F}_p$, and therefore the corresponding character sum has size equal to p .

Proof. This estimate follows from the Riemann Hypothesis for the algebraic curve C over \mathbb{F}_p defined by the Artin-Schreier equation

$$y^p - y = P(x)/Q(x).$$

This was first explicitly stated by Perelmuter in [44], although this was undoubtedly known to Weil; an elementary proof based on Stepanov's method may also be found in [6]. A full proof for all curves using a minimal amount of theory of algebraic curves is found in [2]. \square

Remark 4.3. For our purpose of establishing some non-trivial Type I and Type II estimates for a given choice of σ (and in particular for σ slightly above $1/6$) and for sufficiently small ϖ, δ , it is not necessary to have the full square root cancellation in (4.2), and any power savings of the form p^{1-c} for some fixed $c > 0$ would suffice (with the same dependency on P and Q); indeed, one obtains a non-trivial estimate for a given value of σ once one invokes the q -van der Corput method a sufficient number of times, and once the gains from the cancellation are greater than the losses coming from completion of sums, with the latter becoming negligible in the limit $\varpi, \delta \rightarrow 0$. Such a power saving (with $c = 1/4$) was obtained for the Kloosterman sum (4.3) by Kloosterman [34] using an elementary dilation argument (see also [41] for a generalization), but this argument does not appear to be available for estimates such as (4.4).

In order to prove parts (i), (ii) and (iv) of Theorem 2.8, we need to extend the bounds of Lemma 4.2 in two ways: to sums over $\mathbb{Z}/q\mathbb{Z}$ for q squarefree instead of prime, and to incomplete sums over suitable subsets of $\mathbb{Z}/q\mathbb{Z}$ (the other two parts of the theorem also require exponential sum estimates, but these require the much deeper work of Deligne [9], and will be considered in Section 6).

4.3. Complete exponential sums to squarefree moduli. To extend Lemma 4.2 to squarefree moduli, we first need some preliminaries. We begin with a version of the Chinese Remainder Theorem.

Lemma 4.4 (Chinese Remainder Theorem). *If q_1, q_2 are coprime natural numbers, then for any integer a , or indeed for any $a \in \mathbb{P}^1(\mathbb{Q})$, we have*

$$e_{q_1 q_2}(a) = e_{q_1}\left(\frac{a}{q_2}\right) e_{q_2}\left(\frac{a}{q_1}\right). \quad (4.5)$$

More generally, if q_1, \dots, q_k are pairwise coprime natural numbers, then for any integer a or any $a \in \mathbb{P}^1(\mathbb{Q})$, we have

$$e_{q_1 \dots q_k}(a) = \prod_{i=1}^k e_{q_i}\left(\frac{a}{\prod_{j \neq i} q_j}\right).$$

Proof. It suffices to prove the former claim for $a \in \mathbb{P}^1(\mathbb{Q})$, as the latter then follows by induction.

If a maps to a point at infinity in $\mathbb{P}^1(\mathbb{Z}/q_1 q_2 \mathbb{Z})$, then it must map to a point at infinity in $\mathbb{P}^1(\mathbb{Z}/q_1 \mathbb{Z})$ or $\mathbb{P}^1(\mathbb{Z}/q_2 \mathbb{Z})$, so that both sides of (4.5) are zero.

So we can assume that $a \in \mathbb{Z}/q_1 q_2 \mathbb{Z}$. Let $\overline{q_1}, \overline{q_2}$ be integers such that $q_1 \overline{q_1} = 1 \pmod{q_2}$ and $q_2 \overline{q_2} = 1 \pmod{q_1}$, respectively. Then we have $q_1 \overline{q_1} + q_2 \overline{q_2} = 1 \pmod{q_1 q_2}$, and hence

$$e_{q_1 q_2}(a) = e_{q_1 q_2}(a(q_1 \overline{q_1} + q_2 \overline{q_2})) = e_{q_1 q_2}(q_1 \overline{q_1} a) e_{q_1 q_2}(q_2 \overline{q_2} a).$$

Since $e_{q_1 q_2}(q_1 \overline{q_1} a) = e_{q_2}(\frac{a}{q_1})$ and $e_{q_1 q_2}(q_2 \overline{q_2} a) = e_{q_1}(\frac{a}{q_2})$, the claim follows. \square

If $q \in \mathbb{Z}$ is an integer, we say that q divides f , and write $q|f$, if q divides f in $\mathbb{Z}[X]$. We denote by (q, f) the largest factor of q that divides f (i.e., the positive generator of the ideal of \mathbb{Z} consisting of integers dividing f). Thus for instance $(q, 0) = q$. We also write $f \pmod{q} \in (\mathbb{Z}/q\mathbb{Z})[X]$ for the reduction of f modulo q .

We need the following algebraic lemma, which can be viewed as a version of (a special case of) the fundamental theorem of calculus:

Lemma 4.5. *Let $f = \frac{P}{Q} \in \mathbb{Q}(X)$ with $P, Q \in \mathbb{Z}[X]$ coprime, and let q be a natural number such that $Q \pmod{p}$ is a non-zero polynomial for all primes $p \mid q$ (automatic if Q is monic).*

- (i) *If $q|f'$ and all prime factors of q are sufficiently large depending on the degrees of P and Q , then there exists $c \in \mathbb{Z}/q\mathbb{Z}$ such that $q|f - c$.*
- (ii) *If q is squarefree, if $Q \pmod{p}$ has degree $\deg(Q)$ for all $p \mid q$ and³ $\deg(P) < \deg(Q)$, and if all prime factors of q are sufficiently large depending on the degrees of P and Q , then (q, f') divides (q, f) . In particular, if $(q, f) = 1$ then $(q, f') = 1$.*

³We adopt the convention $\deg(0) = -\infty$.

Proof. We first prove (i). By the Chinese Remainder Theorem, we may assume that $q = p^j$ is the power of a prime. Write $f' = P_1/Q_1$ where P_1 and $Q_1 \in \mathbb{Z}[X]$ are coprime. By definition, the condition $q \mid f'$ implies that $P_1(x) = 0 \pmod{q}$ for all $x \in \mathbb{Z}/q\mathbb{Z}$. On the other hand, since $Q_1 \pmod{p}$ is non-zero in $\mathbb{Z}/p\mathbb{Z}[X]$, the rational function $f' \pmod{q}$ is well-defined at all $x \in \mathbb{Z}/q\mathbb{Z}$ except at most $\deg(Q)$ zeros of Q_1 , and takes the value 0 at all these $\geq q - \deg(Q)$ values. If q is large enough in terms of $\deg(P)$ and $\deg(Q)$, this implies that $f' \pmod{q} = 0 \in \mathbb{Z}/q\mathbb{Z}[X]$, and therefore that $f \pmod{q} = c$ for some $c \in \mathbb{Z}/q\mathbb{Z}$, i.e., that $q \mid f - c$.

Now we prove (ii). If a prime p divides (q, f') , then by (i), there exists $c \in \mathbb{Z}/p\mathbb{Z}$ such that $p \mid f - c$. If $p \nmid (q, f)$, we must have $c \neq 0$. But then $p \mid P - cQ$, where $P - cQ \pmod{p} \in \mathbb{Z}/p\mathbb{Z}[X]$ is (by assumption) a polynomial of degree $\deg(Q) \geq 1$. For $p > \deg(Q)$, this is a contradiction, so that $p \mid (q, f)$. \square

We use this to give an estimate for complete exponential sums, which combines the bounds for Ramanujan sums with those arising from the Riemann Hypothesis for curves.

Proposition 4.6 (Ramanujan-Weil bounds). *Let q be a squarefree natural number, and let $f = \frac{P}{Q} \in \mathbb{Q}(X)$, where $P, Q \in \mathbb{Z}[X]$ are coprime polynomials with Q non-zero modulo p for every $p \mid q$, for instance Q monic. Then we have*

$$\left| \sum_{n \in \mathbb{Z}/q\mathbb{Z}} e_q(f(n)) \right| \leq C^{\Omega(q)} q^{1/2} \frac{(f', q)}{(f'', q)^{1/2}}$$

for some constant $C \geq 1$ depending only on $\deg(P)$ and $\deg(Q)$.

Example 4.7. (1) Let $f(X) := b/X$ for some integer b . We get, after changing the summation variable, a slightly weaker version of the familiar Ramanujan sum bound

$$\left| \sum_{n \in \mathbb{Z}/q\mathbb{Z}} e(bn) \mathbf{1}_{(n, q)=1} \right| \leq (b, q) \tag{4.6}$$

since $(q, f') = (b, q)$ and $(q, f'') = c(b, q)$ in this case for some $c = 1, 2$.

(2) More generally, let $f := a/X + bX$ for some integers a, b . We get a weaker form of Weil's bound for Kloosterman sums

$$\left| \sum_{n \in \mathbb{Z}/q\mathbb{Z}} e_q(a\bar{n} + bn) \mathbf{1}_{(n, q)=1} \right| \leq 2^{\Omega(q)} q^{1/2} \frac{(a, b, q)}{(a, q)^{1/2}},$$

which generalizes (4.3).

Proof. By Lemma 4.4, we can factor the sum as a product of exponential sums over the prime divisors of q :

$$\sum_{n \in \mathbb{Z}/q\mathbb{Z}} e_q(f(n)) = \prod_{p \mid q} \sum_{n \in \mathbb{Z}/p\mathbb{Z}} e_p \left(\frac{f(n)}{(q/p)} \right).$$

Since, for each $p \mid q$, the constant q/p is an invertible element in $\mathbb{Z}/p\mathbb{Z}$, we see that it suffices to prove the estimates

$$\sum_{n \in \mathbb{Z}/p\mathbb{Z}} e_p(f(n)) \ll p, \quad \text{when } p \mid f' \text{ (which implies } p \mid f'') \quad (4.7)$$

$$\sum_{n \in \mathbb{Z}/p\mathbb{Z}} e_p(f(n)) \ll 1, \quad \text{when } p \mid f'' \text{ but } p \nmid f' \quad (4.8)$$

$$\sum_{n \in \mathbb{Z}/p\mathbb{Z}} e_p(f(n)) \ll \sqrt{p}, \quad \text{otherwise,} \quad (4.9)$$

where the implied constants, in all three cases, depend only on $\deg(P)$ and $\deg(Q)$. Thus we may always assume that $p \mid q$ is large enough in terms of $\deg(P)$ and $\deg(Q)$, since otherwise the result is trivial.

The first bound is clear, with implied constant equal to 1. For (4.8), since $p \mid f''$, we conclude from Lemma 4.5 (since p is large enough) that there exists $c \in \mathbb{Z}/p\mathbb{Z}$ such that $p \mid f' - c$. Since $p \nmid f'$, we see that c must be non-zero. Then, since $f' - c = (f - ct)'$, another application of Lemma 4.5 shows that there exists $d \in \mathbb{Z}/p\mathbb{Z}$ such that $p \mid f - ct - d$. This implies that $f(n) = cn + d \pmod{p}$ whenever n is not a pole of $f \pmod{p}$. The denominator Q of f (which is non-zero modulo p by assumption) has at most $\deg(Q)$ zeroes, and therefore we see that $e_p(f(n)) = e_p(cn + d)$ for all but $\leq \deg(Q)$ values of $n \in \mathbb{Z}/p\mathbb{Z}$. Thus (by orthogonality of characters) we get

$$\left| \sum_{n \in \mathbb{Z}/p\mathbb{Z}} e_p(f(n)) \right| = \left| \sum_{n \in \mathbb{Z}/p\mathbb{Z}} e_p(f(n)) - \sum_{n \in \mathbb{Z}/p\mathbb{Z}} e_p(cn + d) \right| \leq \deg(Q).$$

Now we prove (4.9). This estimate follows immediately from Lemma 4.2, except if the reduction $\tilde{f} \in \mathbb{F}_p(X)$ of f modulo p satisfies an identity

$$\tilde{f} = g^p - g + c \quad (4.10)$$

for some $g \in \mathbb{F}_p(X)$ and $c \in \mathbb{F}_p$. We claim that, if p is large enough, this can only happen if $p \mid f'$, which contradicts the assumption of (4.9) and therefore concludes the proof.

To prove the claim, we just observe that if (4.10) holds, then any pole of g would be a pole of \tilde{f} of order p , and thus g must be a polynomial if p is large enough. But then (4.10) implies that $\tilde{f} - c$ either vanishes or has degree at least p . If p is large enough, the latter conclusion is not possible, and thus $p \mid f'$. \square

We also need a variant of the above proposition, which is a slight refinement of an estimate appearing in the proof of [52, Proposition 11]:

Lemma 4.8. *Let d_1, d_2 be squarefree integers, so that $[d_1, d_2]$ is squarefree, and let c_1, c_2, l_1, l_2 be integers. Then there exists $C \geq 1$ such that*

$$\left| \sum_{n \in \mathbb{Z}/[d_1, d_2]\mathbb{Z}} e_{d_1} \left(\frac{c_1}{n + l_1} \right) e_{d_2} \left(\frac{c_2}{n + l_2} \right) \right| \leq C^{\Omega([d_1, d_2])} (c_1, \delta_1) (c_2, \delta_2) (d_1, d_2)$$

where $\delta_i := d_i / (d_1, d_2)$ for $i = 1, 2$.

Proof. As in the proof of Proposition 4.6, we may apply Lemma 4.4 to reduce to the case where $[d_1, d_2] = p$ is a prime number. The bound is then trivial if $(c_1, \delta_1), (c_2, \delta_2)$,

or (d_1, d_2) is equal to p , so we may assume without loss of generality that $d_1 = p$, $d_2 = 1$, and that c_1 is coprime to p . We then need to prove that

$$\sum_{n \in \mathbb{Z}/p\mathbb{Z}} e_p \left(\frac{c_1}{n+l} \right) \ll 1,$$

but this is clear since, by the change of variable $m = c_1/(n+l)$, this sum is just a Ramanujan sum. \square

4.4. Incomplete exponential sums. The bounds in the previous section control “complete” additive exponential sums in one variable in $\mathbb{Z}/q\mathbb{Z}$, by which we mean sums where the variable n ranges over all of $\mathbb{Z}/q\mathbb{Z}$. For our applications, as well as for many others, one needs also to have good estimates for “incomplete” versions of the sums, in which the variable n ranges over an interval, or more generally over the integers weighted by a coefficient sequence which is (shifted) smooth at some scale N .

The most basic technique to obtain such estimates is the method of completion of sums, also called the Pólya-Vinogradov method. In essence, this is an elementary application of discrete Fourier analysis, but the importance of the results cannot be overestimated.

We begin with some facts about the discrete Fourier transform. Given a function

$$f: \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{C}$$

we define its *normalized Fourier transform* $\text{FT}_q(f)$ to be the function on $\mathbb{Z}/q\mathbb{Z}$ given by

$$\text{FT}_q(f)(h) := \frac{1}{q^{1/2}} \sum_{x \in \mathbb{Z}/q\mathbb{Z}} f(x) e_q(hx). \quad (4.11)$$

The normalization factor $1/q^{1/2}$ is convenient because the resulting Fourier transform operator is then unitary with respect to the inner product

$$\langle f, g \rangle := \sum_{x \in \mathbb{Z}/q\mathbb{Z}} f(x) \overline{g(x)}$$

on the space of functions $\mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{C}$. In other words, the Plancherel formula

$$\sum_{x \in \mathbb{Z}/q\mathbb{Z}} f(x) \overline{g(x)} = \sum_{h \in \mathbb{Z}/q\mathbb{Z}} \text{FT}_q(f)(h) \overline{\text{FT}_q(g)(h)}$$

holds for any functions $f, g: \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{C}$. Furthermore, by the orthogonality of additive characters, we have the discrete Fourier inversion formula

$$\text{FT}_q(\text{FT}_q(f))(x) = f(-x)$$

for all $x \in \mathbb{Z}/q\mathbb{Z}$.

Lemma 4.9 (Completion of sums). *Let $M \geq 1$ be a real number and let ψ_M be a function on \mathbb{R} defined by*

$$\psi_M(x) = \psi \left(\frac{x - x_0}{M} \right)$$

where $x_0 \in \mathbb{R}$ and ψ is a smooth function supported on $[c, C]$ satisfying

$$|\psi^{(j)}(x)| \ll \log^{O(1)} M$$

for all fixed $j \geq 0$, where the implied constant may depend on j . Let $q \geq 1$ be an integer, and let

$$M' := \sum_{m \geq 1} \psi_M(m) \ll M(\log M)^{O(1)}.$$

We have:

(i) If $f: \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{C}$ is a function, then

$$\left| \sum_m \psi_M(m) f(m) - \frac{M'}{q} \sum_{m \in \mathbb{Z}/q\mathbb{Z}} f(m) \right| \ll q^{1/2} (\log M)^{O(1)} \sup_{h \in \mathbb{Z}/q\mathbb{Z} \setminus \{0\}} |\text{FT}_q(f)(h)|. \quad (4.12)$$

In particular, if $M \ll q(\log M)^{O(1)}$, then

$$\left| \sum_m \psi_M(m) f(m) \right| \ll q^{1/2} (\log M)^{O(1)} \|\text{FT}_q(f)\|_{\ell^\infty(\mathbb{Z}/q\mathbb{Z})}. \quad (4.13)$$

We also have the variant

$$\begin{aligned} \left| \sum_m \psi_M(m) f(m) - \frac{M'}{q} \sum_{m \in \mathbb{Z}/q\mathbb{Z}} f(m) \right| &\ll (\log M)^{O(1)} \frac{M}{q^{1/2}} \sum_{0 < |h| \leq qM^{-1+\varepsilon}} |\text{FT}_q(f)(h)| \\ &\quad + M^{-A} \sum_{m \in \mathbb{Z}/q\mathbb{Z}} |f(m)| \end{aligned} \quad (4.14)$$

for any fixed $A > 0$ and $\varepsilon > 0$, where the implied constant depends on ε and A .

(ii) If I is a finite index set, and for each $i \in I$, c_i is a complex number and $a_i(q)$ is a residue class, then for each fixed $A > 0$ and $\varepsilon > 0$, one has

$$\begin{aligned} \left| \sum_{i \in I} c_i \sum_m \psi_M(m) \mathbf{1}_{m=a_i(q)} - \frac{M'}{q} \sum_{i \in I} c_i \right| &\ll (\log M)^{O(1)} \frac{M}{q} \sum_{0 < |h| \leq qM^{-1+\varepsilon}} \left| \sum_{i \in I} c_i e_q(a_i h) \right| \\ &\quad + M^{-A} \sum_{i \in I} |c_i|, \end{aligned} \quad (4.15)$$

where the implied constant depends on ε and A .

Remark 4.10. One could relax the derivative bounds on ψ to $|\psi^{(j)}(x)| \ll M^{\varepsilon_j}$ for various small fixed $\varepsilon_j > 0$, at the cost of similarly worsening the various powers of $\log M$ in the conclusion of the lemma to small powers of M , and assuming the ε_j small enough depending on ε and A ; however this variant of the lemma is a little tricky to state, and we will not have use of it here.

Proof. Define the function

$$\psi_{M,q}(x) = \sum_{n \in \mathbb{Z}} \psi_M(x + qn).$$

This is a smooth q -periodic function on \mathbb{R} . By periodization and by the Plancherel formula, we have

$$\sum_m \psi_M(m) f(m) = \sum_{x \in \mathbb{Z}/q\mathbb{Z}} f(x) \psi_{M,q}(x) = \sum_{h \in \mathbb{Z}/q\mathbb{Z}} \text{FT}_q(f)(h) \text{FT}_q(\psi_{M,q})(-h). \quad (4.16)$$

The contribution of the frequency $h = 0$ is given by

$$\text{FT}_q(f)(0) \text{FT}_q(\psi_{M,q})(0) = \frac{1}{q} \sum_{m \in \mathbb{Z}/q\mathbb{Z}} f(m) \sum_{m \in \mathbb{Z}/q\mathbb{Z}} \psi_{M,q}(m) = \frac{M'}{q} \sum_{m \in \mathbb{Z}/q\mathbb{Z}} f(m).$$

We now consider the contribution of the non-zero frequencies. For $h \in \mathbb{Z}/q\mathbb{Z}$, the definition of $\psi_{M,q}$ leads to

$$q^{1/2}\text{FT}_q(\psi_{M,q})(-h) = \Psi\left(\frac{h}{q}\right),$$

where the function Ψ is defined on \mathbb{R}/\mathbb{Z} by

$$\Psi(y) := \sum_m \psi_M(m) e(-my).$$

This is a smooth function $\Psi: \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{C}$. We then have

$$\left| \sum_{h \in \mathbb{Z}/q\mathbb{Z} \setminus \{0\}} \text{FT}_q(f)(h) \text{FT}_q(\psi_{M,q})(-h) \right| \leq \sup_{h \in \mathbb{Z}/q\mathbb{Z} \setminus \{0\}} |\text{FT}_q(f)(h)| q^{-1/2} \sum_{\substack{-q/2 < h \leq q/2 \\ h \neq 0}} \left| \Psi\left(\frac{h}{q}\right) \right|.$$

Applying the Poisson summation formula and the definition $\psi_M(x) = \psi((x - x_0)/M)$, we have

$$\Psi(y) = M \sum_{n \in \mathbb{Z}} \hat{\psi}(M(n + y)) e(-(n + y)x_0)$$

where

$$\hat{\psi}(s) = \int_{\mathbb{R}} \psi(t) e(-st) dt.$$

By repeated integrations by parts, the assumption on the size of the derivatives of ψ gives the bounds

$$|\hat{\psi}(s)| \ll (\log M)^{O(1)} (1 + |s|)^{-A}$$

for any fixed $A \geq 0$, and therefore

$$|\Psi(y)| \ll M (\log M)^{O(1)} (1 + |y|M)^{-A} \quad (4.17)$$

for any fixed $A \geq 0$ and any $-1/2 < y \leq 1/2$. Taking, e.g., $A = 2$, we get

$$\sum_{\substack{-q/2 < h \leq q/2 \\ h \neq 0}} \left| \Psi\left(\frac{h}{q}\right) \right| \ll (\log M)^{O(1)} \sum_{1 \leq h \leq q/2} \frac{M}{(1 + |h|M/q)^2} \ll q (\log M)^{O(1)},$$

and therefore we obtain (4.12). From this, (4.13) follows immediately.

We now turn to (4.14). Fix $A > 0$ and $\varepsilon > 0$. Arguing as above, we have

$$\begin{aligned} \left| \sum_m \psi_M(m) f(m) - \frac{M'}{q} \sum_{m \in \mathbb{Z}/q\mathbb{Z}} f(m) \right| &\leq \frac{1}{q^{1/2}} \sum_{\substack{-q/2 < h \leq q/2 \\ h \neq 0}} \left| \Psi\left(\frac{h}{q}\right) \right| |\text{FT}_q(f)(h)| \\ &\ll (\log M)^{O(1)} \frac{M}{q^{1/2}} \sum_{0 < |h| \leq qM^{-1+\varepsilon}} |\text{FT}_q(f)(h)| \\ &\quad + (\log M)^{O(1)} \sum_{n \in \mathbb{Z}/q\mathbb{Z}} |f(n)| \sum_{|h| > qM^{-1+\varepsilon}} \frac{M}{q(1 + |h|M/q)^A} \end{aligned}$$

Changing A to a large value, we conclude that

$$\left| \sum_m \psi_M(m) f(m) - \frac{M'}{q} \sum_{m \in \mathbb{Z}/q\mathbb{Z}} f(m) \right| \ll M q^{-1/2} (\log M)^{O(1)} \sum_{0 < |h| \leq q M^{-1+\varepsilon}} |\text{FT}_q(f)(h)| + M^{-A} \sum_{n \in \mathbb{Z}/q\mathbb{Z}} |f(n)|,$$

as claimed.

Finally, the claim (ii) follows immediately from (4.14) by setting

$$f(m) := \sum_{\substack{i \in I \\ a_i \equiv m \pmod{q}}} c_i, \quad \text{so that} \quad \text{FT}_q(f)(h) = \frac{1}{\sqrt{q}} \sum_{i \in I} c_i e_q(a_i h).$$

□

Remark 4.11. In Section 7, we will use a slightly refined version where the coefficients $\Psi(h/q)$ above are not estimated trivially.

By combining this lemma with Proposition 4.6, we can obtain non-trivial bounds for incomplete exponential sums of the form

$$\sum_n \psi_N(n) e_q(f(n))$$

for various moduli q , which are roughly of the shape

$$\sum_n \psi_N(n) e_q(f(n)) \ll q^{1/2+\varepsilon}$$

when $N \ll q$. A number of bounds of this type were used by Zhang [52] to obtain his Type I and Type II estimates. However, it turns out that we can improve this bound for certain regimes of q, N when the modulus q is smooth, or at least densely divisible, by using the “ q -van der Corput A -process” of Heath-Brown [25] and Graham-Ringrose [24]. This method was introduced to handle incomplete *multiplicative* character sums, but it is also applicable to incomplete additive character sums. It turns out that these improved estimates lead to significant improvements in the Type I and Type II numerology over that obtained in [52].

Here is the basic estimate on incomplete one-dimensional exponential sums that we will need for the Type I and Type II estimates. Essentially the same bounds were obtained in [28, Theorem 2].

Proposition 4.12 (Incomplete additive character sums). *Let q be a squarefree integer, and let $f = \frac{P}{Q} \in \mathbb{Q}(X)$ with $P, Q \in \mathbb{Z}[X]$, such that the degree of $Q(p)$ is equal to $\deg(Q)$ for all $p \mid q$. Assume that $\deg(P) < \deg(Q)$. Set $q_1 := q/(f, q)$. Let further $N \geq 1$ be given with $N \ll q^{O(1)}$ and let ψ_N be a function on \mathbb{R} defined by*

$$\psi_N(x) = \psi\left(\frac{x - x_0}{N}\right)$$

where $x_0 \in \mathbb{R}$ and ψ is a smooth function with compact support satisfying

$$|\psi^{(j)}(x)| \ll \log^{O(1)} N$$

for all fixed $j \geq 0$, where the implied constant may depend on j .

(i) (*Polyá-Vinogradov + Ramanujan-Weil*) We have the bound

$$\sum_n \psi_N(n) e_q(f(n)) \ll q^\varepsilon \left(q_1^{1/2} + \frac{N}{q_1} \mathbf{1}_{N \geq q_1} \left| \sum_{n \in \mathbb{Z}/q_1 \mathbb{Z}} e_{q_1}(f(n)/(f, q)) \right| \right) \quad (4.18)$$

for any $\varepsilon > 0$. In particular, lifting the $\mathbb{Z}/q_1 \mathbb{Z}$ sum to a $\mathbb{Z}/q \mathbb{Z}$ sum, we have

$$\sum_n \psi_N(n) e_q(f(n)) \ll q^\varepsilon \left(q^{1/2} + \frac{N}{q} \left| \sum_{n \in \mathbb{Z}/q \mathbb{Z}} e_q(f(n)) \right| \right) \quad (4.19)$$

(ii) (*one van der Corput + Ramanujan-Weil*) If $q = rs$, then we have the additional bound

$$\sum_n \psi_N(n) e_q(f(n)) \ll q^\varepsilon \left(\left(N^{1/2} r_1^{1/2} + N^{1/2} s_1^{1/4} \right) + \frac{N}{q_1} \mathbf{1}_{N \geq q_1} \left| \sum_{n \in \mathbb{Z}/q_1 \mathbb{Z}} e_{q_1}(f(n)/(f, q)) \right| \right) \quad (4.20)$$

for any $\varepsilon > 0$, where $r_1 := (r, q_1)$ and $s_1 := (s, q_1)$. In particular, we have

$$\sum_n \psi_N(n) e_q(f(n)) \ll q^\varepsilon \left(\left(N^{1/2} r^{1/2} + N^{1/2} s^{1/4} \right) + \frac{N}{q} \left| \sum_{n \in \mathbb{Z}/q \mathbb{Z}} e_q(f(n)) \right| \right). \quad (4.21)$$

In all cases the implied constants depend on ε , $\deg(P)$, $\deg(Q)$ and the implied constants in the estimates for the derivatives of ψ .

Remark 4.13. The estimates obtained by completion of sums are usually inefficient in the regime $M = o(q)$, and they become trivial for $M \ll q^{1/2}$. For instance, when f is bounded in magnitude by 1, the trivial bound for the right-hand side of (4.13) is q , whereas the trivial bound for the left-hand side is of size about M , which means that one needs a cancellation at least by a factor q/M in the right-hand side to even recover the trivial bound. This becomes a prohibitive restriction if this factor is larger than \sqrt{M} . In this paper, this inefficiency is a major source of loss in our final exponents (the other main source being our frequent reliance on the Cauchy-Schwarz inequality, as each invocation of this inequality tends to halve all gains in exponents arising from application of the Riemann Hypothesis over finite fields). It would thus be of considerable interest to find stronger estimates for incomplete exponential sums. But the only different (general) method we are aware of is the recent “sliding sum method” of Fouvry, Kowalski and Michel [18], which however only improves on the completion technique when M is very close to $q^{1/2}$, and does not give stronger bounds than Lemma 4.9 and Proposition 4.12 in most ranges of interest. (Note however that uniformity of estimates is often even more crucial to obtaining good results, and for this purpose, the completion techniques are indeed quite efficient.)

Proof. We begin with some technical reductions. First of all, we may assume that q has no prime factor smaller than any fixed B depending on $\deg(P)$ and $\deg(Q)$, as the general case then follows by factoring out a bounded factor from q and splitting the summation over n into a bounded number of pieces.

Second, we also observe that, in all cases, we may replace f by $f/(f, q)$ and q by q_1 and (in the case when $q = rs$) r by r_1 and s by s_1 , since if we write $q = q_1 q_2$ we have

$$e_q(f(n)) = e_{q_1} \left(\frac{P(n)}{q_2 Q(n)} \right).$$

Thus we can reduce to a situation where $(f, q) = 1$, so $q = q_1$, $r = r_1$ and $s = s_1$. In this case, the condition $\deg(P) < \deg(Q)$ implies also $(f', q) = (f'', q) = 1$ by Lemma 4.5(ii), provided q has no prime factor less than some constant depending on $\deg(P)$ and $\deg(Q)$, which we may assume to be the case, as we have seen.

We now establish (4.18). We apply (4.14), and put the “main term” with $h = 0$ in the right-hand side, to get

$$\sum_n \psi_N(n) e_q(f(n)) \ll \frac{N^{1+\varepsilon}}{q} \sum_{|h| \leq qN^{-1+\varepsilon}} \left| \sum_{n \in \mathbb{Z}/q\mathbb{Z}} e_q(f(n) + hn) \right| + 1$$

for $\varepsilon > 0$ arbitrarily small (by selecting A large enough in (4.14) using the assumption $N \ll q^{O(1)}$).

If $N < q$, Proposition 4.6 applied for all h gives

$$\sum_n \psi_N(n) e_q(f(n)) \ll \frac{N^{1+\varepsilon}}{q^{1/2}} \sum_{0 \leq |h| \leq qN^{-1+\varepsilon}} (f' + h, q).$$

Since $(f'', q) = 1$, we also have $(f' + h, q) = 1$, and therefore

$$\sum_n \psi_N(n) e_q(f(n)) \ll q^{1/2} N^{2\varepsilon}$$

which implies (4.18). If $N \geq q$, on the other hand, we only apply (4.6) for $h \neq 0$, and we get in the same way

$$\sum_n \psi_N(n) e_q(f(n)) \ll \frac{N^{1+\varepsilon}}{q} \left| \sum_{n \in \mathbb{Z}/q\mathbb{Z}} e_q(f(n)) \right| + q^{1/2} N^{2\varepsilon},$$

which is again (4.18).

Consider now (4.20). We may assume that $N \leq s$, since otherwise the claim follows simply from (4.18), and we may similarly assume that $r \leq N$, since otherwise we can use the trivial bound

$$\sum_n \psi_N(n) e_q(f(n)) \ll N(\log N)^{O(1)} \ll r^{1/2} N^{1/2} (\log N)^{O(1)}.$$

Let $K := \lfloor N/r \rfloor$. Using translation invariance, we can write

$$\sum_n \psi_N(n) e_q(f(n)) = \frac{1}{K} \sum_n \sum_{k=1}^K \psi_N(n + kr) e_q(f(n + kr)).$$

Since $q = rs$, we have

$$e_q(f(n + kr)) = e_r(\bar{s}f(n)) e_s(\bar{r}f(n + kr))$$

by Lemma 4.4 (and periodicity), and hence we obtain

$$\begin{aligned} \left| \sum_n \psi_N(n) e_q(f(n)) \right| &\leq \frac{1}{K} \sum_n \left| \sum_{k=1}^K \psi_N(n + kr) e_s(\bar{r}f(n + kr)) \right| \\ &\ll \frac{N^{1/2}}{K} \left(\sum_n \left| \sum_{k=1}^K \psi_N(n + kr) e_s(\bar{r}f(n + kr)) \right|^2 \right)^{1/2}, \end{aligned}$$

where the factor $N^{1/2}$ arises because the summand is (as a function of n) supported on an interval of length $O(N)$. Expanding the square, we obtain

$$\left| \sum_n \psi_N(n) e_q(f(n)) \right|^2 \ll \frac{N}{K^2} \sum_{1 \leq k, l \leq K} A(k, l), \quad (4.22)$$

where

$$A(k, l) = \sum_n \psi_N(n + kr) \overline{\psi_N(n + lr)} e_s(\bar{r}(f(n + kr) - f(n + lr))).$$

We have

$$A(k, k) = \sum_n |\psi_N(n + kr)|^2 \ll N(\log N)^{O(1)}.$$

and therefore

$$\sum_{1 \leq k \leq K} |A(k, k)| \ll KN(\log N)^{O(1)}. \quad (4.23)$$

There remains to handle the off-diagonal terms. For each $k \neq l$, we have

$$\frac{f(n + kr) - f(n + lr)}{r} = g(n)$$

where $g = P_1/Q_1 \in \mathbb{Q}(X)$ with integral polynomials

$$\begin{aligned} P_1(X) &= P(X + kr)Q(X + lr) - Q(X + kr)P(X + lr), \\ Q_1(X) &= rQ(X + kr)Q(X + lr). \end{aligned}$$

Note that P_1 and Q_1 satisfy the assumptions of (4.18) with respect to the modulus s (although they might not be coprime).

We now claim that (provided all prime factors of q are large enough) we have

$$(s, g') \mid (s, k - l) \quad \text{and} \quad (s, g) \mid (s, k - l).$$

Indeed, since $\deg(P) < \deg(Q)$ and the degree of the reduction of Q modulo primes dividing q is constant, it is enough to show that $(s, g) \mid (s, k - l)$ by Lemma 4.5(ii). So suppose that a prime p divides (s, g) . Then, by change of variable we have

$$p \mid (s, f(X + (k - l)r) - f(X)).$$

By induction, we thus have

$$p \mid (s, f(X + i(k - l)r) - f(X))$$

for any integer i . If $p \nmid k - l$, then $(k - l)r$ generates $\mathbb{Z}/p\mathbb{Z}$ as an additive group, and we conclude that $p \mid (s, f(X + a) - f(X))$ for all $a \in \mathbb{Z}/p\mathbb{Z}$. This implies that $f \pmod{p}$ is constant where it is defined. But since $\deg(P) < \deg(Q)$ holds modulo p , for p large enough in terms of $\deg(Q)$, this would imply that $p \mid f$ (as in Lemma 4.5(ii)), contradicting the assumption $(s, f) = 1$. Thus we have $p \mid k - l$, and we conclude $(s, g) \mid (s, k - l)$, and then $(s, g') \mid (s, k - l)$, as claimed.

By (4.18) and Proposition 4.6, we have

$$\begin{aligned} A(k, l) &\ll q^\varepsilon \left(s^{1/2} + \frac{N}{s} \mathbf{1}_{N \geq s/(s, k-l)} \right) \left| \sum_{n \in \mathbb{Z}/s\mathbb{Z}} e_s(g(n)) \right| \\ &\ll q^\varepsilon \left(s^{1/2} + \frac{N}{s^{1/2}} (s, k - l)^{1/2} \mathbf{1}_{N \geq s/(s, k-l)} \right). \end{aligned}$$

Summing over k and l , we have

$$\sum_{1 \leq k \neq l \leq K} |A(k, l)| \ll q^\varepsilon K^2 s^{1/2} + q^\varepsilon N s^{-1/2} \sum_{1 \leq k \neq l \leq K} (s, k-l)^{1/2} \mathbf{1}_{N \geq s/(s, k-l)}. \quad (4.24)$$

We use the simple bound

$$\mathbf{1}_{N \geq s/(s, k-l)} \leq \sqrt{(s, k-l)} \sqrt{\frac{N}{s}}$$

to estimate the last sum as follows:

$$\begin{aligned} N s^{-1/2} \sum_{1 \leq k \neq l \leq K} (s, k-l)^{1/2} \mathbf{1}_{N \geq s/(s, k-l)} &\leq \frac{N^{3/2}}{s} \sum_{1 \leq k \neq l \leq K} (s, k-l) \\ &\ll N^{3/2} s^{-1} \times K^2 q^\varepsilon \ll K^2 s^{1/2} q^\varepsilon \end{aligned}$$

using Lemma 1.4 and the bound $N < s$. We combine this with (4.23) and (4.24) in the bound (4.22) to obtain

$$\left| \sum_n \psi_N(n) e_q(f(n)) \right|^2 \ll q^\varepsilon \frac{N}{K^2} \left(K N (\log N)^{O(1)} + K^2 s^{1/2} \right) \ll q^\varepsilon (N r + N s^{1/2}),$$

from which (4.20) follows. \square

Remark 4.14. (1) Assuming that $(f, q) = 1$, the first bound (4.18) is non-trivial (i.e., better than $O(N)$) as long as N is a bit larger than $q^{1/2}$. As for (4.20), we see that in the regime where the factorization $q = rs$ satisfies $r \approx q^{1/3} \approx s^{1/2}$, the bound is non-trivial in the significantly wider range where N is a bit larger than $q^{1/3}$.

(2) The procedure can also be generalized with similar results to more general q -periodic functions than $n \mapsto e_q(f(n))$, and this will be important for the most advanced Type I estimates (see Section 6.10.1).

Remark 4.15. One can iterate the above argument and show that

$$\begin{aligned} \left| \sum_n \psi_N(n) e_q(f(n)) \right| &\ll q^\varepsilon \left(\sum_{i=1}^{l-1} N^{1-1/2^i} \tilde{r}_i^{1/2^i} + N^{1-1/2^{l-1}} \tilde{r}_l^{1/2^l} \right. \\ &\quad \left. + \frac{N}{q_1} \mathbf{1}_{N \geq q_1} \left| \sum_{n \in \mathbb{Z}/q_1 \mathbb{Z}} e_{q_1}(f(n)/(f, q)) \right| \right) \end{aligned}$$

for any fixed $l \geq 1$ and any factorization $q = r_1 \dots r_l$, with $\tilde{r}_i = (r_i, q_1)$; see [24], [28]. However, we have found in practice that taking l to be 3 or higher (corresponding to two or more applications of the q -van der Corput A -process) ends up being counterproductive, mainly because the power of q that one can save over the trivial bound decays exponentially in l . However, it is possible that some other variation of the arguments (for instance, taking advantage of the Parseval identity, which would be a q -analogue of the van der Corput B -process) may give further improvements.

In our particular application, we only need a special case of the above proposition. This is a strengthening of [52, Lemma 11], and it shows how an assumption of dense divisibility of a modulus may be exploited in estimates for exponential sums.

Corollary 4.16. *Let $N \geq 1$ and let ψ_N be a function on \mathbb{R} defined by*

$$\psi_N(x) = \psi\left(\frac{x - x_0}{N}\right)$$

where $x_0 \in \mathbb{R}$ and ψ is a smooth function with compact support satisfying

$$|\psi^{(j)}(x)| \ll \log^{O(1)} N$$

for all fixed $j \geq 0$, where the implied constant may depend on j .

Let d_1, d_2 be squarefree integers, not necessarily coprime. Let c_1, c_2, l_1, l_2 be integers. Let $y \geq 1$ be a real number, and suppose that $[d_1, d_2]$ is y -densely divisible. Let d be a divisor of $[d_1, d_2]$ and let $a \pmod{d}$ be any residue class.

If $N \leq [d_1, d_2]^{O(1)}$, then we have

$$\left| \sum_{n=a \pmod{d}} \psi_N(n) e_{d_1}\left(\frac{c_1}{n+l_1}\right) e_{d_2}\left(\frac{c_2}{n+l_2}\right) \right| \ll [d_1, d_2]^\varepsilon \left(d^{-1/2} N^{1/2} [d_1, d_2]^{1/6} y^{1/6} + d^{-1} \frac{(c_1, \delta'_1)}{\delta'_1} \frac{(c_2, \delta'_2)}{\delta'_2} N \right),$$

for any $\varepsilon > 0$, where $\delta_i := d_i/(d_1, d_2)$ and $\delta'_i := \delta_i/(d, \delta_i)$ for $i = 1, 2$. We also have the variant bound

$$\left| \sum_{n=a \pmod{d}} \psi_N(n) e_{d_1}\left(\frac{c_1}{n+l_1}\right) e_{d_2}\left(\frac{c_2}{n+l_2}\right) \right| \ll [d_1, d_2]^\varepsilon \left(d^{-1/2} [d_1, d_2]^{1/2} + d^{-1} \frac{(c_1, \delta'_1)}{\delta'_1} \frac{(c_2, \delta'_2)}{\delta'_2} N \right).$$

In both cases the implied constant depends on ε .

Proof. Denote $q = [d_1, d_2]$. We first consider the case $d = 1$, so that the congruence condition $n = a \pmod{d}$ is vacuous. Since $R = y^{1/3} q^{1/3} \leq yq$, the dense divisibility hypothesis implies that there exists a factorization $q = rs$ for some integers r, s such that

$$y^{-2/3} q^{1/3} \leq r \leq y^{1/3} q^{1/3}$$

and

$$y^{-1/3} q^{2/3} \leq s \leq y^{2/3} q^{2/3}.$$

Note now that, by the Chinese Remainder Theorem (as in Lemma 4.4), we can write

$$e_{d_1}\left(\frac{c_1}{n+l_1}\right) e_{d_2}\left(\frac{c_2}{n+l_2}\right) = e_q(f(n))$$

for a rational function $f = P/Q \in \mathbb{Q}(X)$ satisfying the assumptions of Proposition 4.12 (in particular $\deg(P) < \deg(Q)$). The first bound follows immediately from Proposition 4.12(ii), combined with the complete sum estimate

$$\left| \sum_{n \in \mathbb{Z}/[d_1, d_2]\mathbb{Z}} e_{d_1}\left(\frac{c_1}{n+l_1}\right) e_{d_2}\left(\frac{c_2}{n+l_2}\right) \right| \ll q^\varepsilon (c_1, \delta_1)(c_2, \delta_2)(d_1, d_2)$$

of Lemma 4.8. The second bound similarly follows from Proposition 4.12(i).

Now we consider the case when $d > 1$. Making the substitution $n = n'd + a$ and applying the previous argument (with N replaced by N/d , and with suitable modifications to x_0 and f), we reduce to showing that

$$\left| \sum_{n \in \mathbb{Z}/[d_1, d_2]\mathbb{Z}: n=a \pmod{d}} e_{d_1} \left(\frac{c_1}{n+l_1} \right) e_{d_2} \left(\frac{c_2}{n+l_2} \right) \right| \ll q^\varepsilon(c_1, \delta'_1)(c_2, \delta'_2)(d'_1, d'_2)$$

where $d'_i := d_i/(d, d_i)$ for $i = 1, 2$ (note that $\frac{d(d'_1, d'_2)}{[d_1, d_2]} = \frac{1}{\delta'_1 \delta'_2}$). However, this again follows from Lemma 4.8 after making the change of variables $n = n'd + a$. \square

5. TYPE I AND TYPE II ESTIMATES

Using the estimates of the previous section, we can now prove the Type I and Type II results of Theorem 2.8, with the exception of part (iii) of that theorem in which we only make a preliminary reduction for now. The rest of the proof of that part, which depends on the concepts and results of Section 6, will be found in Section 8.

We recall the statements (see Definition 2.6).

Theorem 5.1 (New Type I and Type II estimates). *Let $\varpi, \delta, \sigma > 0$ be fixed quantities, let I be a bounded subset of \mathbb{R} , let $i \geq 1$ be fixed, let $a \pmod{(P_I)}$ be a primitive congruence class, and let $M, N \gg 1$ be quantities with*

$$MN \asymp x \tag{5.1}$$

and

$$x^{1/2-\sigma} \ll N \ll x^{1/2}. \tag{5.2}$$

Let α, β be coefficient sequences located at scales M, N respectively, with β satisfying the Siegel-Walfisz property. Then we have the estimate

$$\sum_{\substack{d \in \mathcal{D}_I^{(i)}(x^\delta) \\ d \ll x^{1/2+2\varpi}}} |\Delta(\alpha \star \beta; a \pmod{d})| \ll x \log^{-A} x \tag{5.3}$$

for any fixed $A > 0$, provided that one of the following hypotheses holds:

- (i) $i = 1$, $54\varpi + 15\delta + 5\sigma < 1$, and $N \ll x^{1/2-2\varpi-c}$ for some fixed $c > 0$.
- (ii) $i = 2$, $56\varpi + 16\delta + 4\sigma < 1$, and $N \ll x^{1/2-2\varpi-c}$ for some fixed $c > 0$.
- (iii) $i = 4$, $\frac{160}{3}\varpi + 16\delta + \frac{34}{9}\sigma < 1$, $64\varpi + 18\delta + 2\sigma < 1$, and $N \ll x^{1/2-2\varpi-c}$ for some fixed $c > 0$.
- (iv) $i = 1$, $68\varpi + 14\delta < 1$, and $N \gg x^{1/2-2\varpi-c}$ for some sufficiently small fixed $c > 0$.

The proof of the case (iii) uses the general form of the Riemann Hypothesis over finite fields [9], but the proofs of (i), (ii), (iv) only need the Riemann Hypothesis for curves over finite fields.

Before we begin the rigorous proof of Theorem 5.1, we give an informal sketch of our strategy of proof for these estimates, which is closely modeled on the arguments of Zhang [52]. The basic idea is to reduce the estimate (5.3) to a certain exponential sum estimate, of the type found in Corollary 4.16 (and, for the estimate (iii), in Corollary 6.24 of the next section). The main tools for these reductions are completion of sums (Lemma 4.9), the triangle inequality, and many techniques related to the Cauchy-Schwarz inequality (viewed in a broad sense), for instance Vinogradov's bilinear form method, the q -van

der Corput A -process, the method of Weyl differencing, or the dispersion method of Linnik.

5.1. Bilinear form estimates. We begin with a short discussion of typical instances of applications of the Cauchy-Schwarz inequality (some examples already appeared in previous sections). We want to estimate a sum

$$\sum_{s \in S} c_s$$

of (typically) complex numbers c_s indexed by some finite set S of large size. Suppose we can parameterize S (possibly with repetition) by a *non-trivial* product set $A \times B$, i.e., by a product where neither factor is too small, or otherwise prove an inequality

$$\left| \sum_{s \in S} c_s \right| \leq \left| \sum_{a \in A} \sum_{b \in B} \alpha_a \beta_b k_{a,b} \right|$$

for certain coefficients α_a , β_b and $k_{a,b}$. The crucial insight is that one can often derive non-trivial estimates for an expression of this type with little knowledge of the coefficients α_a , β_b , by exploiting the bilinear structure and studying the coefficients $k_{a,b}$.

Precisely, one can apply the Cauchy-Schwarz inequality to bound the right-hand side by

$$\left(\sum_{a \in A} |\alpha_a|^2 \right)^{1/2} \left(\sum_{a \in A} \left| \sum_{b \in B} \beta_b k_{a,b} \right|^2 \right)^{1/2}.$$

The first factor in the above expression is usually easy to estimate, and the second factor can be expanded as

$$\left| \sum_{b, b' \in B} \beta_b \overline{\beta_{b'}} C(b, b') \right|^{1/2}, \quad C(b, b') = \sum_{a \in A} k_{a,b} \overline{k_{a,b'}}.$$

One can then distinguish between the *diagonal contribution* defined by $b = b'$ and the *off-diagonal contribution* where $b \neq b'$. The contribution of the former is

$$\sum_{b \in B} \sum_{a \in A} |\beta_b|^2 |k_{a,b}|^2$$

which is (usually) not small, since there cannot be cancellation between these non-negative terms. It may however be estimated satisfactorily, provided B is large enough for the diagonal $\{(b, b) : b \in B\}$ to be a “small” subset of the square $B \times B$. (In practice, there might be a larger subset of $B \times B$ than the diagonal where the coefficient $C(b, b')$ is not small, and that is then incorporated in the diagonal; in this paper, where b and b' are integers, it is the size of a $\gcd(b - b', q)$ that will dictate which terms can be considered diagonal).

On the other hand, the individual off-diagonal terms $C(b, b')$ can be expected to exhibit cancellation that makes them individually small. In order for the sum over $b \neq b'$ to remain of manageable size, one needs B to remain not too large. In order to balance the two contributions, it turns out to be extremely useful to have a flexible *family* of parameterizations $(a, b) \mapsto s$ of S by product sets $A \times B$, so that one can find a parameterization for which the set B is close to the optimum size arising from various estimates of the diagonal and non-diagonal parts. This idea of flexibility is a key idea

at least since Iwaniec's discovery [29] of the bilinear form of the error term in the linear sieve.

One of the key ideas in Zhang's paper [52] is that if one is summing over smooth moduli, then such a flexible range of factorizations exists; to put it another way, the restriction to smooth moduli is essentially a “well-factorable” weight in the sense of Iwaniec. In this paper, we isolated the key property of smooth moduli needed for such arguments, namely the property of *dense divisibility*. The general strategy is thus to keep exploiting the smoothness or dense divisibility of the moduli to split the sums over such moduli into a “well-factorable” form to which the Cauchy-Schwarz inequality may be profitably applied. (Such a strategy was already used to optimize the use of the q -van der Corput A -process in Corollary 4.16.)

5.2. Sketch of proofs. We now give a more detailed, but still very informal, sketch of the proof of Theorem 5.1, omitting some steps and some terms for sake of exposition (e.g., smooth cutoffs are not mentioned). For simplicity we will pretend that the quantities ϖ, δ are negligible, although the quantity σ will still be of a significant size (note from Lemma 2.7 that we will eventually need to take σ to be at least $1/10$). The first step is to exploit the dense divisibility of the modulus d to factor it as $d = qr$, with q, r located at certain scales Q, R which we will specify later; with ϖ negligible, we expect QR to be approximately equal to $x^{1/2}$ but a bit larger. Our task is then to obtain a non-trivial bound on the quantity

$$\sum_{q \asymp Q} \sum_{r \asymp R} |\Delta(\alpha \star \beta; a(qr))|,$$

or equivalently to obtain a non-trivial bound on

$$\sum_{q \asymp Q} \sum_{r \asymp R} c_{q,r} \Delta(\alpha \star \beta; a(qr))$$

for an arbitrary bounded sequence $c_{q,r}$. We suppress here, and later, some additional information on the moduli q, r , e.g. that they are squarefree and coprime, to simplify this informal exposition. For similar reasons we are being vague on what a “non-trivial bound” means, but roughly speaking, it should improve upon the “trivial bound” by a factor of $\log^{-A} x$ where A is very large (or arbitrarily large).

If we insert the definition (1.1), and denote generically by EMT the contribution of the second term in that definition (which is the “expected main term”), we see that we need a non-trivial bound on the quantity

$$\sum_{q \asymp Q} \sum_{r \asymp R} c_{q,r} \sum_{n=a(qr)} \alpha \star \beta(n) - \text{EMT}.$$

For simplicity, we will handle the r averaging trivially, and thus seek to control the sum

$$\sum_{q \asymp Q} c_{q,r} \sum_{n=a(qr)} \alpha \star \beta(n) - \text{EMT}$$

for a single $r \asymp R$. We rearrange this as

$$\sum_{m \asymp M} \alpha(m) \sum_{q \asymp Q} c_{q,r} \sum_{\substack{n \asymp N \\ nm=a(qr)}} \beta(n) - \text{EMT}.$$

Note that for fixed m coprime with q , the number of pairs (q, n) with $q \asymp Q$, $n \asymp N$, and $nm = a(qr)$ is expected to be about $\frac{QN}{QR} = \frac{N}{R}$. Thus, if we choose R to be a little bit less than N , e.g. $R = x^{-\varepsilon}N$, then the number of pairs (q, n) associated to a given value of m is expected to be non-trivial. This opens up the possibility of using the dispersion method of Linnik [37], as the diagonal contribution in that method is expected to be negligible. Accordingly, we apply Cauchy-Schwarz in the variable m , eliminating the rough coefficient sequence α , and end up with the task of controlling an expression of the shape

$$\sum_{m \asymp M} \left| \sum_{q \asymp Q} c_{q,r} \sum_{\substack{n \asymp N \\ nm=a(qr)}} \beta(n) - \text{EMT} \right|^2.$$

Opening the square as sketched above, this is equal to

$$\sum_{q_1, q_2 \asymp Q} c_{q_1, r} \overline{c_{q_2, r}} \sum_{n_1, n_2 \asymp N} \beta(n_1) \overline{\beta(n_2)} \left(\sum_{\substack{m \asymp M \\ n_1 m = a(q_1 r) \\ n_2 m = a(q_2 r)}} 1 - \text{EMT} \right).$$

Note that, since $a(qr)$ is a primitive residue class, the constraints $n_1 m = a(q_1 r)$, $n_2 m = a(q_2 r)$ imply $n_1 = n_2 (r)$. Thus we can write $n_2 = n_1 + \ell r$ for some $\ell = O(N/R)$, which will be rather small (compare with the method of Weyl differencing).

For simplicity, we consider only⁴ the case $\ell = 0$ here. We are thus led to the task of controlling sums such as

$$\sum_{q_1, q_2 \asymp Q} c_{q_1, r} \overline{c_{q_2, r}} \sum_{n \asymp N} \beta(n) \overline{\beta(n)} \left(\sum_{\substack{m \asymp M \\ nm=a(q_1 r) \\ nm=a(q_2 r)}} 1 - \text{EMT} \right). \quad (5.4)$$

It turns out (using a technical trick of Zhang which we will describe below) that we can ensure that the moduli q_1, q_2 appearing here are usually coprime, in the sense that the contribution of the non-coprime pairs q_1, q_2 are negligible. Assuming this, we can use the Chinese Remainder Theorem to combine the two constraints $nm = a(q_1 r)$, $nm = a(q_2 r)$ into a single constraint $nm = a(q_1 q_2 r)$ on m . Now, we note that if R is slightly less than N , then (since MN is close to x , and QR is close to $x^{1/2}$) the modulus $q_1 q_2 r$ is comparable to M . This means that the inner sum

$$\sum_{\substack{m \asymp M \\ nm=a(q_1 q_2 r)}} 1 - \text{EMT}$$

is essentially a complete sum, and can therefore be very efficiently handled by Lemma 4.9. This transforms (5.4) into expressions such as

$$\sum_{0 < |h| \leq H} c_h \sum_{q_1, q_2 \asymp Q} c_{q_1, r} \overline{c_{q_2, r}} \sum_{n \asymp N} \beta(n) \overline{\beta(n)} e_{q_1 q_2 r} \left(\frac{ah}{n} \right),$$

where $H \approx \frac{Q^2 R}{M}$ is a fairly small quantity, and the coefficients c_h are bounded. At this point, the contribution of the zero frequency $h = 0$ has cancelled out with the expected main term EMT (up to negligible error).

⁴Actually, for technical reasons, in the rigorous argument we will dispose of the $\ell = 0$ contribution by a different method, so the discussion here should be viewed as an oversimplification.

This expression involves the essentially unknown (but bounded) coefficients $c_{q_1,r}$, $c_{q_2,r}$, $\beta(n)$, and as before, we can not do much more than eliminate them using the Cauchy-Schwarz inequality. This can be done in several ways here, depending on which variables are taken “outside” of the Cauchy-Schwarz inequality. For instance, if we take n to eliminate the $\beta(n)\overline{\beta(n)}$ term, one is led, after expanding the square and exchanging the sum in the second factor of the Cauchy-Schwarz inequality, to expressions such as

$$\sum_{0 < |h_1|, |h_2| \leq H} \sum_{q_1, q_2, s_1, s_2 \asymp Q} \sum_{n \asymp N} \left| \sum_{n \asymp N} e_{q_1 q_2 r} \left(\frac{ah_1}{n} \right) e_{s_1 s_2 r} \left(-\frac{ah_2}{n} \right) \right|.$$

The sum over n has length N close to the modulus $[q_1 q_2 r, s_1 s_2 r] \approx Q^4 R$, and therefore can be estimated non-trivially using Corollary 4.16. As we will see, this arrangement of the Cauchy-Schwarz inequality is sufficient to establish the Type II estimate (iv).

The Type I estimates are obtained by a slightly different application of Cauchy-Schwarz. Indeed, note for instance that as the parameter σ (which occurs in the Type I condition, but not in Type II) gets larger, the length N in the sum may become smaller in comparison to the modulus $q_1 q_2 s_1 s_2 r$ in the exponential sum

$$\sum_{n \asymp N} e_{q_1 q_2 r} \left(\frac{ah_1}{n} \right) e_{s_1 s_2 r} \left(-\frac{ah_2}{n} \right),$$

and this necessitates more advanced exponential sum estimates to recover non-trivial cancellation. Here, the q -van der Corput A -method enlarges the range of parameters for which we can prove that such a cancellation occurs. This is one of the main reasons why our Type I estimates improve on those in [52]. (The other main reason is that we will adjust the Cauchy-Schwarz inequality to lower the modulus in the exponential sum to be significantly smaller than $q_1 q_2 s_1 s_2 r \asymp Q^4 R$, while still keeping both the diagonal and off-diagonal components of the Cauchy-Schwarz estimate under control.)

5.3. Reduction to exponential sums. We now turn to the details of the above strategy. We begin with the preliminary manipulations (mostly following [52]) to reduce the estimate (5.3) to a certain exponential sum estimate. This reduction can be done simultaneously in the four cases (i), (ii), (iii), (iv), but the verification of the exponential sum estimate requires a different argument in each of the four cases.

In the remainder of this section $\varpi, \delta, \sigma, I, i, a, M, N, \alpha, \beta$ are as in Theorem 5.1. First of all, since β satisfies the Siegel-Walfisz property, the Bombieri-Vinogradov Theorem 2.9 implies

$$\sum_{d \leq x^{1/2} \log^{-B} x} |\Delta(\alpha \star \beta; a(d))| \ll x \log^{-A} x \quad (5.5)$$

for any fixed $A > 0$ and some B depending on A . From this and dyadic decomposition, we conclude that to prove (5.3), it suffices to establish the estimate

$$\sum_{d \in \mathcal{D}_I^{(i)}(x^\delta) \cap [D, 2D]} |\Delta(\alpha \star \beta; a(d))| \ll x \log^{-A} x$$

for any fixed $A > 0$, and for all D such that

$$x^{1/2} \ll D \ll x^{1/2+2\varpi} \quad (5.6)$$

(recall that this means $x^{1/2} \ll x^{o(1)} D$ and $D \ll x^{1/2+2\varpi+o(1)}$ for any $\varepsilon > 0$).

We now fix one such D . In the spirit of [52], we first restrict d to moduli which do not have too many small prime factors. Precisely, let

$$D_0 := \exp(\log^{1/3} x), \quad (5.7)$$

and let $\mathcal{E}(D)$ be the set of $d \in [D, 2D]$ such that

$$\prod_{\substack{p|d \\ p \leq D_0}} p > \exp(\log^{2/3} x). \quad (5.8)$$

We have (cf. [11, lemme 4]):

Lemma 5.2. *For any fixed $A > 0$, and D obeying (5.6), we have*

$$|\mathcal{E}(D)| \ll D \log^{-A} x.$$

Proof. If $d \geq 1$ satisfies (5.8), then

$$\prod_{\substack{p|d \\ p \leq D_0}} p > \exp(\log^{2/3} x) = D_0^{\log^{1/3} x}.$$

In particular, d has at least $\log^{1/3} x$ prime factors, and therefore

$$\tau(d) \geq 2^{\log^{1/3} x}.$$

On the other hand, we have

$$\sum_{\substack{D \leq d \leq 2D \\ \tau(d) \geq \kappa}} 1 \leq \frac{1}{\kappa} \sum_{D \leq d \leq 2D} \tau(d) \ll \frac{D}{\kappa} \log x$$

for any $\kappa > 0$ by the standard bound

$$\sum_{D \leq d \leq 2D} \tau(d) \ll D \log x$$

(see (1.3)), and the result follows. \square

This allows us to dispose of these exceptional moduli:

Corollary 5.3. *We have*

$$\sum_{\substack{d \in \mathcal{D}_I^{(i)}(x^\delta) \\ d \in \mathcal{E}(D)}} |\Delta(\alpha \star \beta; a(d))| \ll x \log^{-A} x$$

for any fixed $A > 0$.

Proof. From (1.4) we derive the trivial bound

$$|\Delta(\alpha \star \beta; a(d))| \ll x D^{-1} \tau(d)^{O(1)} \log^{O(1)} x,$$

for every $d \asymp D$, and hence the Cauchy-Schwarz inequality gives

$$\sum_{\substack{d \in \mathcal{D}_I^{(i)}(x^\delta) \\ d \in \mathcal{E}(D)}} |\Delta(\alpha \star \beta; a(d))| \ll |\mathcal{E}(D)|^{1/2} x D^{-1} \log^{O(1)} x \left(\sum_{d \in \mathcal{E}(D)} \tau(d)^{O(1)} \right)^{1/2} \ll x \log^{-A} x$$

by Lemma 5.2 and (1.3). \square

It therefore suffices to show that

$$\sum_{\substack{d \in \mathcal{D}_I^{(i)}(x^\delta) \\ d \in [D, 2D] \setminus \mathcal{E}(D)}} |\Delta(\alpha \star \beta; a(d))| \ll x \log^{-A} x \quad (5.9)$$

for any fixed $A > 0$.

Let $\varepsilon > 0$ be a small fixed quantity to be chosen later. From (5.2) and (5.6) we have

$$1 \leq x^{-3\varepsilon} N \leq D$$

for x large enough. Let $j \geq 0$ and $k \geq 0$ be fixed integers so that

$$i - 1 = j + k \quad (5.10)$$

Then any integer $d \in \mathcal{D}_I^{(i)}(x^\delta)$ can by definition (see Definition 2.1) be factored as $d = qr$, where $q \in \mathcal{D}_I^{(j)}(x^\delta)$, $r \in \mathcal{D}_I^{(k)}(x^\delta)$, and

$$x^{-3\varepsilon-\delta} N \leq r \leq x^{-3\varepsilon} N.$$

Remark 5.4. The reason that r is taken to be slightly less than N is to ensure that a diagonal term is manageable when the time comes to apply the Cauchy-Schwarz inequality. The factor of 3 in the exponent is merely technical, and should be ignored on a first reading (ε will eventually be set to be very small, so the constants in front of ε will ultimately be irrelevant).

Let $d \in [D, 2D] \setminus \mathcal{E}(D)$, so that

$$s = \prod_{\substack{p|d \\ p \leq D_0}} p \ll 1.$$

Then replacing q by $q/(q, s)$ and r by $r(q, s)$, we obtain a factorization $d = qr$ where q has no prime factor $\leq D_0$ and

$$x^{-3\varepsilon-\delta} N \ll r \ll x^{-3\varepsilon} N. \quad (5.11)$$

By Lemma 2.10(0), (i), we have

$$q \in \mathcal{D}^{(j)}(sx^\delta) = \mathcal{D}^{(j)}(x^{\delta+o(1)}), \quad r \in \mathcal{D}^{(k)}(sx^\delta) = \mathcal{D}^{(k)}(x^{\delta+o(1)}).$$

In particular, $q \in \mathcal{D}_J^{(j)}(x^{\delta+o(1)})$ where $J := I \cap (D_0, +\infty)$. As $i \geq 1$, we also have $qr = d \in \mathcal{D}_I(x^\delta) = \mathcal{D}_I^{(1)}(x^\delta)$.

Remark 5.5. The reason for removing all the small prime factors from q will become clearer later, when the Cauchy-Schwarz inequality is invoked to replace the single parameter q with two parameters q_1, q_2 in the same range. By excluding the small primes from q_1, q_2 , this will ensure that q_1 and q_2 will almost always be coprime, which will make things much simpler.

The next step is to perform dyadic decompositions of the range of the q and r variables, which (in view of (5.1)) reduces the proof of (5.9) to the proof of the estimates

$$\sum_{\substack{q \in \mathcal{D}_J^{(j)}(x^{\delta+o(1)}) \cap [Q, 2Q] \\ r \in \mathcal{D}_I^{(k)}(x^{\delta+o(1)}) \cap [R, 2R] \\ qr \in \mathcal{D}_I(x^\delta)}} |\Delta(\alpha \star \beta; a(qr))| \ll MN \log^{-A} x$$

for any fixed $A > 0$ and any Q, R obeying the conditions

$$x^{-3\varepsilon-\delta}N \ll R \ll x^{-3\varepsilon}N, \quad (5.12)$$

$$x^{1/2} \ll QR \ll x^{1/2+2\varpi}. \quad (5.13)$$

We note that these inequalities also imply that

$$NQ \ll x^{1/2+2\varpi+\delta+3\varepsilon}. \quad (5.14)$$

For future reference we also claim the bound

$$RQ^2 \ll x. \quad (5.15)$$

In the cases (i)-(iii) of Theorem 5.1, we have $\sigma + 4\varpi + \delta < \frac{1}{2}$ (with plenty of room to spare), and (5.15) then easily follows from (5.12), (5.13), (5.2). For case (i), we have $6\varpi + \delta < \frac{1}{2}$, and we may argue as before, but with (5.2) replaced by the bound $N \gg x^{1/2-2\varpi-c}$.

Let Q, R be as above. We will abbreviate

$$\sum_q A_q = \sum_{q \in \mathcal{D}_J^{(j)}(x^{\delta+o(1)}) \cap [Q, 2Q]} A_q \quad (5.16)$$

and

$$\sum_r A_r = \sum_{r \in \mathcal{D}_I^{(k)}(x^{\delta+o(1)}) \cap [R, 2R]} A_r \quad (5.17)$$

for any summands A_q, A_r .

We now split the discrepancy by writing

$$\Delta(\alpha \star \beta; a(qr)) = \Delta_1(\alpha \star \beta; a(qr)) + \Delta_2(\alpha \star \beta; a(qr))$$

where

$$\begin{aligned} \Delta_1(\alpha \star \beta; a(qr)) &:= \sum_{n=a(qr)} (\alpha \star \beta)(n) - \frac{1}{\varphi(q)} \sum_{\substack{(n,q)=1 \\ n=a(r)}} (\alpha \star \beta)(n), \\ \Delta_2(\alpha \star \beta; a(qr)) &:= \frac{1}{\varphi(q)} \sum_{\substack{(n,q)=1 \\ n=a(r)}} (\alpha \star \beta)(n) - \frac{1}{\varphi(qr)} \sum_{(n,qr)=1} (\alpha \star \beta)(n). \end{aligned}$$

The second term can be dealt with immediately:

Lemma 5.6. *We have*

$$\sum_{q,r: qr \in \mathcal{D}_I(x^\delta)} |\Delta_2(\alpha \star \beta; a(qr))| \ll NM \log^{-A} x$$

for any fixed $A > 0$.

Proof. Since $r \leq 2R \ll x^{1/2+o(1)-3\varepsilon}$, the Bombieri-Vinogradov Theorem 2.9, applied for each q to $\alpha_q \star \beta_q$, where $\alpha_q = \alpha \mathbf{1}_{(n,q)=1}$, $\beta_q = \beta \mathbf{1}_{(n,q)=1}$, gives

$$\sum_{\substack{R \leq r \leq 2R \\ qr \in \mathcal{D}_I(x^\delta)}} \left| \sum_{\substack{(n,q)=1 \\ n=a(r)}} (\alpha \star \beta)(n) - \frac{1}{\varphi(r)} \sum_{(n,qr)=1} (\alpha \star \beta)(n) \right| \ll NM \log^{-A} x,$$

since β_q inherits the Siegel-Walfisz property from β . Dividing by $\varphi(q)$ and summing over $q \leq 2Q$, we get the result using the standard estimate

$$\sum_q \frac{1}{\varphi(q)} \ll \log x.$$

□

To deal with Δ_1 , it is convenient to define

$$\Delta_0(\alpha \star \beta; a, b_1, b_2) = \sum_{\substack{n=a \pmod{r} \\ n=b_1 \pmod{q}}} (\alpha \star \beta)(n) - \sum_{\substack{n=a \pmod{r} \\ n=b_2 \pmod{q}}} (\alpha \star \beta)(n)$$

for all integers a, b_1, b_2 coprime to P_I . Indeed, we have

$$\sum_{\substack{q,r \\ qr \in \mathcal{D}_I(x^\delta)}} |\Delta_1(\alpha \star \beta; a, qr)| \leq \frac{1}{\varphi(P_I)} \sum_{\substack{b \pmod{P_I} \\ (b, P_I)=1}} \sum_{\substack{q,r \\ qr \in \mathcal{D}_I(x^\delta)}} |\Delta_0(\alpha \star \beta; a, a, b)|$$

by the triangle inequality and the Chinese Remainder Theorem. Hence it is enough to prove that

$$\sum_{\substack{q,r \\ qr \in \mathcal{D}_I(x^\delta)}} |\Delta_0(\alpha \star \beta; a, b_1, b_2)| \ll NM \log^{-A} x \quad (5.18)$$

for all a, b_1, b_2 coprime to P_I , and this will be our goal. The advantage of this step is that the two terms in Δ_0 behave symmetrically, in contrast to those in Δ_1 (or Δ), and this will simplify the presentation of the dispersion method: in the notation of [3, 37, 52], one only needs to control \mathcal{S}_1 , and one avoids dealing explicitly with \mathcal{S}_2 or \mathcal{S}_3 . This is mostly an expository simplification, however, since the estimation of \mathcal{S}_1 is always the most difficult part in applications of the dispersion method.

The fact that $r \leq R$ is slightly less than N ensures that the constraint $n = a \pmod{r}$ leaves room for non-trivial averaging of the variable n , and allows us to profitably use the dispersion method of Linnik. We begin by writing

$$\sum_{\substack{q,r \\ qr \in \mathcal{D}_I(x^\delta)}} |\Delta_0(\alpha \star \beta; a, b_1, b_2)| = \sum_{\substack{q,r \\ qr \in \mathcal{D}_I(x^\delta)}} c_{q,r} \left(\sum_{\substack{n=a \pmod{r} \\ n=b_1 \pmod{q}}} (\alpha \star \beta)(n) - \sum_{\substack{n=a \pmod{r} \\ n=b_2 \pmod{q}}} (\alpha \star \beta)(n) \right)$$

where $c_{q,r}$ are complex numbers of modulus 1. Expanding the Dirichlet convolution and exchanging the sums, we obtain

$$\sum_{\substack{q,r \\ qr \in \mathcal{D}_I(x^\delta)}} |\Delta_0(\alpha \star \beta; a, b_1, b_2)| = \sum_r \sum_m \alpha(m) \left(\sum_{\substack{mn=a \pmod{r} \\ qr \in \mathcal{D}_I(x^\delta)}} c_{q,r} \beta(n) (\mathbf{1}_{mn=b_1 \pmod{q}} - \mathbf{1}_{mn=b_2 \pmod{q}}) \right).$$

By the Cauchy-Schwarz inequality applied to the r and m sums, (2.4), (2.6) and Lemma 1.3 we have

$$\begin{aligned} \sum_{\substack{q,r \\ qr \in \mathcal{D}_I(x^\delta)}} |\Delta_0(\alpha \star \beta; a, b_1, b_2)| &\leq R^{1/2} M^{1/2} (\log x)^{O(1)} \left(\sum_r \sum_m \psi_M(m) \right. \\ &\quad \times \left. \left| \sum_{\substack{mn=a \pmod{r} \\ qr \in \mathcal{D}_I(x^\delta)}} c_{q,r} \beta(n) (\mathbf{1}_{mn=b_1 \pmod{q}} - \mathbf{1}_{mn=b_2 \pmod{q}}) \right|^2 \right)^{1/2} \end{aligned}$$

for any smooth coefficient sequence ψ_M at scale M such that $\psi_M(m) \geq 1$ for m in the support of β . This means in particular that it is enough to prove the estimate

$$\sum_r \sum_m \psi_M(m) \left| \sum_{\substack{mn=a \ (r) \\ qr \in \mathcal{D}_I(x^\delta)}} c_{q,r} \beta(n) (\mathbf{1}_{mn=b_1 \ (q)} - \mathbf{1}_{mn=b_2 \ (q)}) \right|^2 \ll N^2 M R^{-1} \log^{-A} x \quad (5.19)$$

for any fixed $A > 0$, where ψ_M is a smooth coefficient sequence at scale M .

Let Σ denote the left-hand side of (5.19). Expanding the square, we find

$$\Sigma = \Sigma(b_1, b_1) - \Sigma(b_1, b_2) - \Sigma(b_2, b_1) + \Sigma(b_2, b_2), \quad (5.20)$$

where

$$\Sigma(b_1, b_2) := \sum_r \sum_m \psi_M(m) \sum_{\substack{q_1, q_2, n_1, n_2 \\ mn_1 = mn_2 = a \ (r) \\ q_1 r, q_2 r \in \mathcal{D}_I(x^\delta)}} c_{q_1, r} \overline{c_{q_2, r}} \beta(n_1) \overline{\beta(n_2)} \mathbf{1}_{mn_1 = b_1 \ (q_1)} \mathbf{1}_{mn_2 = b_2 \ (q_2)}$$

for any integers b_1 and b_2 coprime to P_I (where the variables q_1 and q_2 are subject to the constraint (5.16)). We will prove that

$$\Sigma(b_1, b_2) = X + O(N^2 M R^{-1} \log^{-A} x) \quad (5.21)$$

for all b_1 and b_2 , where the main term X is independent of b_1 and b_2 . From (5.20), the desired conclusion (5.19) then follows.

Since a is coprime to qr , so are the variables n_1 and n_2 in the sum. In particular, they satisfy the congruence $n_1 = n_2 \ (r)$. We write $n_2 = n_1 + \ell r$ in the sum, rename n_1 as n , and therefore obtain

$$\begin{aligned} \Sigma(b_1, b_2) &= \sum_r \sum_\ell \sum_{\substack{q_1, q_2 \\ q_1 r, q_2 r \in \mathcal{D}_I(x^\delta)}} c_{q_1, r} \overline{c_{q_2, r}} \sum_n \beta(n) \overline{\beta(n + \ell r)} \\ &\quad \sum_m \psi_M(m) \mathbf{1}_{mn = b_1 \ (q_1)} \mathbf{1}_{m(n + \ell r) = b_2 \ (q_2)} \mathbf{1}_{mn = a \ (r)} \end{aligned}$$

after some rearranging (remembering that $(n, q_1 r) = (n + \ell r, q_2 r) = 1$). Note that the sum over ℓ is restricted to a range $0 \leq |\ell| \ll L := N R^{-1}$.

We will now complete the sum in m (which is long since M is just a bit smaller than the modulus $[q_1, q_2]r \leq Q^2 R$) using Lemma 4.9 (ii), but first we handle separately the diagonal case $n_1 = n_2$, i.e., $\ell = 0$. This contribution, say $T(b_1, b_2)$, satisfies

$$\begin{aligned} |T(b_1, b_2)| &\leq \sum_r \sum_{\substack{q_1, q_2 \\ q_1 r, q_2 r \in \mathcal{D}_I(x^\delta)}} \sum_n |\beta(n)|^2 \sum_m \psi_M(m) \mathbf{1}_{mn = b_1 \ (q_1)} \mathbf{1}_{mn = b_2 \ (q_2)} \mathbf{1}_{mn = a \ (r)} \\ &\ll \sum_{r \asymp R} \sum_{q_1, q_2 \asymp Q} \sum_{s \asymp x} \tau(s) \mathbf{1}_{s = b_1 \ (q_1)} \mathbf{1}_{s = b_2 \ (q_2)} \mathbf{1}_{s = a \ (r)} \\ &\ll \sum_{r \asymp R} \sum_{q_1, q_2 \asymp Q} \frac{x}{r [q_1, q_2]} \ll x \ll N^2 M R^{-1} \log^{-A} x \end{aligned}$$

(since $RQ^2 \ll x$ (from (5.15)) and $R \ll x^{-3\epsilon} N$).

Now we consider the contributions where $\ell \neq 0$. First, since n and $n + \ell r$ are coprime to $q_1 r$ and $q_2 r$ respectively, we have

$$\mathbf{1}_{mn = b_1 \ (q_1)} \mathbf{1}_{m(n + \ell r) = b_2 \ (q_2)} \mathbf{1}_{mn = a \ (r)} = \mathbf{1}_{m = \gamma \ ([q_1, q_2]r)} \quad (5.22)$$

for some residue class $\gamma \pmod{[q_1, q_2]r}$ (which depends on b_1, b_2, ℓ, n and a). We will denote $q_0 = (q_1, q_2)$, and observe that since q_1, q_2 have no prime factor less than D_0 , we have either $q_0 = 1$ or $q_0 \geq D_0$. (The first case gives the principal contribution, and the reader may wish to assume that $q_0 = 1$ in a first reading.) The sum over n is further restricted by the congruence

$$\frac{b_1}{n} = \frac{b_2}{n + \ell r} \pmod{q_0}, \quad (5.23)$$

and we will use

$$C(n) := \mathbf{1}_{\frac{b_1}{n} = \frac{b_2}{n + \ell r} \pmod{q_0}} \quad (5.24)$$

to denote the characteristic function of this condition (taking care of the fact that it depends on other parameters). Observe that, since q_0 is coprime to rb_1 , this is the characteristic function of a union of at most $(b_1 - b_2, q_0, \ell rb_1) \leq (q_0, \ell)$ congruence classes modulo q_0 .

By Lemma 4.9 (ii) applied to each choice of q_1, q_2, r, ℓ (where I is the range of the remaining parameter n) and summing, we derive

$$\Sigma(b_1, b_2) = \Sigma_0(b_1, b_2) + \Sigma_1(b_1, b_2) + O(MN^2 R^{-1} \log^{-A} x),$$

where

$$\Sigma_0(b_1, b_2) := \left(\sum_m \psi_M(m) \right) \sum_r r^{-1} \sum_{\ell \neq 0} \sum_{q_1, q_2} \frac{c_{q_1, r} \overline{c_{q_2, r}}}{[q_1, q_2]} \sum_n \beta(n) \overline{\beta(n + \ell r)} C(n)$$

$q_1 r, q_2 r \in \mathcal{D}_I(x^\delta)$

and

$$\Sigma_1(b_1, b_2) \ll 1 + x^\varepsilon \hat{\Sigma}_1(b_1, b_2)$$

with

$$\hat{\Sigma}_1(b_1, b_2) := \sum_r \sum_{\ell \neq 0} \sum_{q_1, q_2} \sum_{q_1 r, q_2 r \in \mathcal{D}_I(x^\delta)} c_{q_1, r} \overline{c_{q_2, r}} \frac{1}{H} \sum_{1 \leq |h| \leq H} \left| \sum_n \beta(n) \overline{\beta(n + \ell r)} C(n) e_{[q_1, q_2]r}(\gamma h) \right|,$$

where $H := x^\varepsilon [q_1, q_2] r M^{-1} \ll x^\varepsilon Q^2 R M^{-1}$. We caution that H depends on q_1 and q_2 , so one has to take some care if one is to interchange the h and q_1, q_2 summations.

Remark 5.7. Before going further, note that H is rather small since M and R are close to $x^{1/2}$ and $\varepsilon > 0$ will be very small: precisely, we have

$$H \ll H_0 := x^\varepsilon \times (QR)^2 \times \frac{N}{R} \times \frac{1}{NM}$$

and using (5.12), (5.13), (5.1), we see that

$$x^{4\varepsilon} \ll H_0 \ll x^{4\varpi + \varepsilon} (N/R) \ll x^{4\varpi + \delta + 4\varepsilon}. \quad (5.25)$$

As we will be using small values of $\varpi, \delta, \varepsilon$, one should thus think of H as being quite small compared to x .

We can deal immediately with $\Sigma_0(b_1, b_2)$. We distinguish between the contributions of q_1 and q_2 which are coprime, and the remainder. The first is independent of b_1 and b_2

(since these parameters are only involved in the factor $C(n) = \mathbf{1}_{b_1/n=b_2/(n+\ell r)}(q_0)$, which is then always 1) and it will be the main term X , thus

$$X := \left(\sum_m \psi_M(m) \right) \sum_r r^{-1} \sum_{\ell \neq 0} \sum_{\substack{q_1, q_2 \\ q_1 r, q_2 r \in \mathcal{D}_I(x^\delta) \\ (q_1, q_2)=1}} \frac{c_{q_1, r} \overline{c_{q_2, r}}}{[q_1, q_2]} \sum_n \beta(n) \overline{\beta(n + \ell r)}.$$

The remaining contribution to $\Sigma_0(b_1, b_2)$, say $\Sigma'_0(b_1, b_2)$, satisfies

$$\Sigma'_0(b_1, b_2) \ll \frac{M(\log x)^{O(1)}}{R} \sum_{r \asymp R} \sum_{|\ell| \ll L} \sum_{\substack{1 \neq q_0 \leq Q \\ q_0 \in \mathcal{S}_J}} \frac{1}{q_0} \sum_{q_1, q_2 \asymp Q/q_0} \frac{1}{q_1 q_2} \sum_n (\tau(n) \tau(n + \ell r))^{O(1)} C(n).$$

We rearrange to sum over ℓ first (remember that $C(n)$ depends on ℓ also). Since rb_1 is coprime with q_0 , the condition $b_1/n = b_2/(n + \ell r) \pmod{q_0}$ is a congruence condition modulo q_0 for ℓ , and therefore

$$\sum_{|\ell| \ll L} \tau(n + \ell r)^{O(1)} \mathbf{1}_{b_1/n=b_2/(n+\ell r)}(q_0) \ll \left(1 + \frac{L}{q_0}\right) \log^{O(1)} x = \left(1 + \frac{N}{q_0 R}\right) \log^{O(1)} x$$

by Lemma 1.3. Since all $q_0 \neq 1$ in the sum satisfy $D_0 \leq q_0 \ll Q$, we get

$$\begin{aligned} \Sigma'_0(b_1, b_2) &\ll \frac{MN(\log x)^{O(1)}}{R} \sum_{r \asymp R} \sum_{D_0 \leq q_0 \leq Q} \frac{1}{q_0} \left(1 + \frac{N}{q_0 R}\right) \sum_{q_1, q_2 \asymp Q/q_0} \frac{1}{q_1 q_2} \\ &\ll MN \log^{O(1)} x \sum_{D_0 \leq q_0 \leq Q} \frac{1}{q_0} \left(1 + \frac{N}{q_0 R}\right) \\ &\ll MN \log^{O(1)} x + \frac{1}{D_0} \frac{MN^2}{R} \log^{O(1)} x \\ &\ll MN^2 R^{-1} \log^{-A} x, \end{aligned}$$

since $R \ll x^{-3\varepsilon} N$ and $D_0 \gg \log^A x$ for all $A > 0$.

Hence we have shown that

$$\Sigma(b_1, b_2) = X + O(x^\varepsilon |\hat{\Sigma}_1(b_1, b_2)|) + O(MN^2 R^{-1} \log^{-A} x). \quad (5.26)$$

From the definition, and in particular the localization of r and the value of H , we have

$$\begin{aligned} |\hat{\Sigma}_1(b_1, b_2)| &\leq \sum_r \sum_{\ell \neq 0} \sum_{\substack{q_1, q_2 \\ q_1 r, q_2 r \in \mathcal{D}_I(x^\delta)}} \frac{1}{H} \sum_{0 < |h| \leq H} \left| \sum_n C(n) \beta(n) \overline{\beta(n + \ell r)} e_{[q_1, q_2]r}(\gamma h) \right| \\ &\ll x^{-\varepsilon} \frac{M}{RQ^2} \sum_{1 \leq |\ell| \ll L} \sum_{q_0 \leq Q} q_0 \sum_r \Upsilon_{\ell, r}(b_1, b_2; q_0) \end{aligned} \quad (5.27)$$

where q_0 is again (q_1, q_2) and

$$\begin{aligned} \Upsilon_{\ell, r}(b_1, b_2; q_0) &:= \sum_{\substack{q_1, q_2 \asymp Q/q_0 \\ (q_1, q_2)=1}} \sum_{\substack{q_0 q_1, q_0 q_2 \in \mathcal{D}_I^{(j)}(x^{\delta+o(1)}) \\ q_0 q_1 r, q_0 q_2 r \in \mathcal{D}_I(x^\delta)}} \mathbf{1}_{b_1/n=b_2/(n+\ell r)}(q_0) \\ &\quad \sum_{1 \leq |h| \ll \frac{x^\varepsilon RQ^2}{q_0 M}} \left| \sum_n C(n) \beta(n) \overline{\beta(n + \ell r)} \Phi_\ell(h, n, r, q_0, q_1, q_2) \right|. \end{aligned} \quad (5.28)$$

The latter expression involves the phase function Φ_ℓ , which we define for parameters $\mathbf{p} = (h, n, r, q_0, q_1, q_2)$ by

$$\Phi_\ell(\mathbf{p}) := e_r \left(\frac{ah}{nq_0q_1q_2} \right) e_{q_0q_1} \left(\frac{b_1h}{nrq_2} \right) e_{q_2} \left(\frac{b_2h}{(n + \ell r)rq_0q_1} \right). \quad (5.29)$$

Here we have spelled out and split, using (5.22) and the Chinese Remainder Theorem, the congruence class of γ modulo $[q_1, q_2]r$, and changed variables so that q_1 is q_0q_1 , q_2 is q_0q_2 (hence $[q_1, q_2]r$ becomes $q_0q_1q_2r$). Moreover, the r summation must be interpreted using (5.17). It will be important for later purposes to remark that we also have

$$\hat{\Sigma}_1(b_1, b_2) = 0$$

unless

$$\frac{x^\varepsilon Q^2 R}{q_0 M} \gg 1, \quad (5.30)$$

since otherwise the sum over h is empty.

Gathering these estimates, we obtain the following general reduction statement, where we pick a suitable value of (j, k) in each of the four cases of Theorem 5.1:

Theorem 5.8 (Exponential sum estimates). *Let $\varpi, \delta, \sigma > 0$ be fixed quantities, let I be a bounded subset of \mathbb{R} , let $j, k \geq 0$ be fixed, let $a(P_I), b_1(P_I), b_2(P_I)$ be primitive congruence classes, and let $M, N \gg 1$ be quantities satisfying the conditions (5.1) and (5.2). Let $\varepsilon > 0$ be a sufficiently small fixed quantity, and let Q, R be quantities obeying (5.12), (5.13). Let ℓ be an integer with $1 \leq |\ell| \ll N/R$, and let β be a coefficient sequence located at scale N .*

Let $\Phi_\ell(\mathbf{p})$ be the phase function defined by (5.29) for parameters $\mathbf{p} = (h, n, r, q_0, q_1, q_2)$, let $C(n)$ be the cutoff (5.24) and let $\Upsilon_{\ell, r}(b_1, b_2; q_0)$ be defined in terms of β, Φ, C by (5.28). Then we have

$$\sum_r \Upsilon_{\ell, r}(b_1, b_2; q_0) \ll x^{-\varepsilon} Q^2 R N(q_0, \ell) q_0^{-2} \quad (5.31)$$

for all $q_0 \in \mathcal{S}_I$, where the sum over r is over $r \in \mathcal{D}_I^{(k)}(x^{\delta+o(1)}) \cap [R, 2R]$, provided that one of the following hypotheses is satisfied:

- (i) $(j, k) = (0, 0)$, $54\varpi + 15\delta + 5\sigma < 1$, and $N \ll x^{1/2-2\varpi-c}$ for some fixed $c > 0$.
- (ii) $(j, k) = (1, 0)$, $56\varpi + 16\delta + 4\sigma < 1$, and $N \ll x^{1/2-2\varpi-c}$ for some fixed $c > 0$.
- (iii) $(j, k) = (1, 2)$, $\frac{160}{3}\varpi + 16\delta + \frac{34}{9}\sigma < 1$, $64\varpi + 18\delta + 2\sigma < 1$, and $N \ll x^{1/2-2\varpi-c}$ for some fixed $c > 0$.
- (iv) $(j, k) = (0, 0)$, $68\varpi + 14\delta < 1$, and $N \gg x^{1/2-2\varpi-c}$ for some sufficiently small fixed $c > 0$.

The proof of the estimate (iii) requires Deligne's form of the Riemann Hypothesis for algebraic varieties over finite fields, but the proofs of (i), (ii), (iv) do not.

Indeed, inserting this bound in (5.27) we obtain

$$x^\varepsilon |\hat{\Sigma}(b_1, b_2)| \ll x^{-\varepsilon} M N \sum_{q_0 \ll Q} \frac{1}{q_0} \sum_{1 \leq |\ell| \ll NR^{-1}} (q_0, \ell) \ll x^{-\varepsilon} M N^2 R^{-1}$$

(by Lemma 1.4, crucially using the fact that we have previously removed the $\ell = 0$ contribution), and hence using (5.26), we derive the goal (5.21).

Remark 5.9. As before, one should consider the $q_0 = 1$ case as the main case, so that the technical factors of q_0 , (ℓ, q_0) , and $C(n)$ should be ignored at a first reading; in practice, we will usually (though not always) end up discarding several powers of q_0 in the denominator in the final bounds for the $q_0 > 1$ case. The trivial bound for $\Upsilon_{\ell,r}(b_1, b_2; q_0)$ is about $(Q/q_0)^2 NH$ with $H = x^\varepsilon RQ^2 M^{-1} q_0^{-1}$. Thus one needs to gain about H over the trivial bound. As observed previously, H is quite small, and even a modestly non-trivial exponential sum estimate can suffice for this purpose (after using Cauchy-Schwarz to eliminate factors such as $\beta(n)\beta(n + \ell r)$).

It remains to establish Theorem 5.8 in the four cases indicated. We will do this for (i), (ii), (iv) below, and defer the proof of (iii) to Section 8. In all four cases, one uses the Cauchy-Schwarz inequality to eliminate non-smooth factors such as $\beta(n)$ and $\beta(n + \ell r)$, and reduces matters to incomplete exponential sum estimates. In the cases (i), (ii), (iv) treated below, the one-dimensional exponential sum estimates from Section 4.4 suffice; for the final case (iii), a multidimensional exponential sum estimate is involved, and we will prove it using Deligne's formalism of the Riemann Hypothesis over finite fields, which we survey in Section 6.

5.4. Proof of Type II estimate. We begin with the proof of Theorem 5.8(iv), which is the simplest of the four estimates to prove. We fix notation and hypotheses as in this statement.

To prove (5.31), we will not exploit any averaging in the variable r , and more precisely, we will show that

$$\Upsilon_{\ell,r}(b_1, b_2; q_0) \ll x^{-\varepsilon} Q^2 N(q_0, \ell) q_0^{-2} \quad (5.32)$$

for each $q_0 \geq 1$, $r = R$ and $\ell \ll N/R$. We abbreviate $\Upsilon = \Upsilon_{\ell,r}(b_1, b_2; q_0)$ in the remainder of this section and denote

$$H = x^\varepsilon RQ^2 M^{-1} q_0^{-1}.$$

By (5.28), we can then write

$$\Upsilon = \sum_{\substack{q_1, q_2 \asymp Q/q_0 \\ (q_1, q_2) = 1}} \sum_{1 \leq |h| \leq H} \sum_{n} c_{h, q_1, q_2} \sum_n C(n) \beta(n) \overline{\beta(n + \ell r)} \Phi_\ell(h, n, r, q_0, q_1, q_2) \quad (5.33)$$

for some coefficients c_{h, q_1, q_2} with modulus at most 1. We then exchange the order of summation to move the sum over n (and the terms $C(n)\beta(n)\overline{\beta(n + \ell r)}$) outside. Since $C(n)$ is the characteristic function of at most (q_0, ℓ) congruence classes modulo q_0 (as observed after (5.23)), we have

$$\sum_n C(n) |\beta(n)|^2 |\beta(n + \ell r)|^2 \ll N \frac{(q_0, \ell)}{q_0} \quad (5.34)$$

by (1.3) (and the Cauchy-Schwarz inequality), using the fact that $Q \leq N$.

By another application of the Cauchy-Schwarz inequality, and after inserting (by positivity) a suitable coefficient sequence $\psi_N(n)$, smooth at scale N and ≥ 1 for n in

the support of $\beta(n)\overline{\beta(n+\ell r)}$, we conclude the bound

$$\begin{aligned} |\Upsilon|^2 &\ll N \frac{(q_0, \ell)}{q_0} \sum_n \psi_N(n) C(n) \left| \sum_{\substack{q_1, q_2 \asymp Q/q_0 \\ (q_1, q_2)=1}} \sum_{1 \leq |h| \leq H} c_{h, q_1, q_2} \Phi_\ell(h, n, r, q_0, q_1, q_2) \right|^2 \\ &\ll N \frac{(q_0, \ell)}{q_0} \sum_{\substack{q_1, q_2, s_1, s_2 \asymp Q/q_0 \\ (q_1, q_2)=(s_1, s_2)=1}} \cdots \sum_{1 \leq h_1, h_2 \leq |H|} |S_{\ell, r}(h_1, h_2, q_1, q_2, s_1, s_2)|, \end{aligned}$$

where the exponential sum $S_{\ell, r} = S_{\ell, r}(h_1, h_2, q_1, q_2, s_1, s_2)$ is given by

$$S_{\ell, r} := \sum_n C(n) \psi_N(n) \Phi_\ell(h_1, n, r, q_0, q_1, q_2) \overline{\Phi_\ell(h_2, n, r, q_0, s_1, s_2)}. \quad (5.35)$$

We will prove below the following estimate for this exponential sum (compare with [52, (12.5)]):

Proposition 5.10. *For any*

$$\mathbf{p} = (h_1, h_2, q_1, q_2, s_1, s_2)$$

with $(q_0 q_1 q_2 s_1 s_2, r) = 1$, any $\ell \neq 0$ and r as above with

$$q_0 q_i, \quad q_0 s_i \ll Q, \quad r \ll R,$$

we have

$$|S_{\ell, r}(\mathbf{p})| \ll (q_0, \ell) \left(q_0^{-2} Q^2 R^{1/2} + \frac{N}{q_0 R} (h_1 s_1 s_2 - h_2 q_1 q_2, r) \right).$$

Assuming this, we obtain

$$|\Upsilon|^2 \ll N \left(\frac{(q_0, \ell)}{q_0} \right)^2 \sum_{\substack{q_1, q_2, s_1, s_2 \asymp Q/q_0 \\ (q_1, q_2)=(s_1, s_2)=1}} \cdots \sum_{1 \leq h_1, h_2 \leq |H|} \left(\frac{1}{q_0} Q^2 R^{1/2} + \frac{N}{R} (h_1 s_1 s_2 - h_2 q_1 q_2, r) \right)$$

(since $S_{\ell, r} = 0$ unless $(q_0 q_1 q_2 s_1 s_2, r) = 1$, by the definition (5.29) and the definition of e_q in Section 4).

Making the change of variables $\Delta = h_1 s_1 s_2 - h_2 q_1 q_2$, and noting that each Δ has at most $\tau_3(\Delta) = |\{(a, b, c) : abc = \Delta\}|$ representations in terms of h_2, q_1, q_2 for each fixed h_1, s_1, s_2 , we have

$$\begin{aligned} \sum_{\substack{q_1, q_2, s_1, s_2 \asymp Q/q_0 \\ (q_1, q_2)=(s_1, s_2)=1}} \cdots \sum_{1 \leq h_1, h_2 \leq |H|} (h_1 s_1 s_2 - h_2 q_1 q_2, r) &\leq \sum_{|\Delta| \ll H(Q/q_0)^2} (\Delta, r) \sum_{h_1, s_1, s_2} \tau_3(h_1 s_1 s_2 - \Delta) \\ &\ll H \left(\frac{Q}{q_0} \right)^2 \sum_{0 \leq |\Delta| \ll H(Q/q_0)^2} (\Delta, r) \\ &\ll H \left(\frac{Q}{q_0} \right)^2 \left(\frac{H Q^2}{q_0^2} + R \right) \end{aligned}$$

by Lemma 1.3 (bounding $\tau_3 \leq \tau^2$) and Lemma 1.4. Therefore we obtain

$$\begin{aligned}
|\Upsilon|^2 &\ll N \frac{(q_0, \ell)^2}{q_0^2} \left\{ \frac{H^2 Q^2 R^{1/2}}{q_0} \left(\frac{Q}{q_0} \right)^4 + \frac{H^2 N}{R} \left(\frac{Q}{q_0} \right)^4 + NH \left(\frac{Q}{q_0} \right)^2 \right\} \\
&\ll \frac{N^2 Q^4 (q_0, \ell)^2}{q_0^4} \left\{ \frac{H^2 Q^2 R^{1/2}}{N} + \frac{H^2}{R} + \frac{H}{Q^2} \right\} \\
&\ll \frac{N^2 Q^4 (q_0, \ell)^2}{q_0^4} \left\{ x^{2\varepsilon} \frac{Q^6 R^{5/2}}{M^2 N} + x^{2\varepsilon} \frac{R Q^4}{M^2} + \frac{x^\varepsilon R}{M} \right\}
\end{aligned} \tag{5.36}$$

where we have discarded some powers of $q_0 \geq 1$ in the denominator to reach the second and third lines. We now observe that

$$\begin{aligned}
\frac{Q^6 R^{5/2}}{M^2 N} &\asymp \frac{(NQ)(QR)^5}{x^2 R^{5/2}} \ll \frac{x^{1+12\varpi+\delta+3\varepsilon}}{R^{5/2}} \ll \frac{x^{1+12\varpi+7\delta/2+21\varepsilon/2}}{N^{5/2}} \\
\frac{Q^4 R}{M^2} &\asymp \frac{N^2 R Q^4}{x^2} = \frac{(QR)(NQ)^3}{x^2 N} \ll \frac{x^{8\varpi+3\delta+9\varepsilon}}{N} \\
\frac{R}{M} &\asymp \frac{NR}{x} \ll x^{-1-3\varepsilon} N^2 \ll x^{-3\varepsilon}
\end{aligned}$$

by (5.13) and (5.14) and $N \ll M$. Under the Type II assumption that $N \gg x^{1/2-2\varpi-c}$ for a small enough $c > 0$ and that $\varepsilon > 0$ is small enough, we see that (5.36) implies (5.32) provided ϖ and δ satisfy

$$\begin{cases} 1 + 12\varpi + \frac{7\delta}{2} < \frac{5}{2}(\frac{1}{2} - 2\varpi) \\ 8\varpi + 3\delta < \frac{1}{2} - 2\varpi \end{cases} \Leftrightarrow \begin{cases} 68\varpi + 14\delta < 1 \\ 20\varpi + 6\delta < 1, \end{cases}$$

both of which are, indeed, consequences of the hypotheses of Theorem 5.8 (iv) (the first implies the second because $\varpi > 0$ so $\delta < 1/14$).

To finish this treatment of the Type II sums, it remains to prove the proposition.

Proof of Proposition 5.10. For fixed $(r, \ell, q_0, a, b_1, b_2)$ we can use (5.29) to express the phase Φ_ℓ in the form

$$\Phi_\ell(h, n, r, q_0, q_1, q_2) = e_r^{(1)}\left(\frac{h}{q_1 q_2 n}\right) e_{q_0 q_1}^{(2)}\left(\frac{h}{n q_2}\right) e_{q_2}^{(3)}\left(\frac{h}{(n + \tau) q_0 q_1}\right)$$

where $e_d^{(i)}$ denotes various non-trivial additive characters modulo d which may depend on $(r, \ell, q_0, a, b_1, b_2)$ and $\tau = \ell r$.

We denote $\Phi_1(n) = \Phi_\ell(h_1, n, r, q_0, q_1, q_2)$ and $\Phi_2(n) = \Phi_\ell(h_2, n, r, q_0, s_1, s_2)$, and thus we have

$$\begin{aligned}
\Phi_1(n) \overline{\Phi_2(n)} &= e_r^{(1)}\left(\frac{h_1}{q_1 q_2 n} - \frac{h_2}{s_1 s_2 n}\right) e_{q_0 q_1}^{(2)}\left(\frac{h_1}{n q_2}\right) e_{q_0 s_1}^{(2)}\left(-\frac{h_2}{n s_2}\right) \\
&\quad e_{q_2}^{(3)}\left(\frac{h_1}{(n + \tau) q_0 q_1}\right) e_{s_2}^{(3)}\left(-\frac{h_2}{(n + \tau) q_0 s_1}\right)
\end{aligned} \tag{5.37}$$

and this can be written

$$\Phi_1(n) \overline{\Phi_2(n)} = e_{d_1}^{(4)}\left(\frac{c_1}{n}\right) e_{d_2}^{(5)}\left(\frac{c_2}{n + \tau}\right)$$

where

$$d_1 := r q_0 [q_1, s_1], \quad d_2 := [q_2, s_2]$$

for some c_1 and c_2 .

Now, since $C(n)$ is the characteristic function of $\leq (q_0, \ell)$ residue classes modulo q_0 , we deduce

$$|S_{\ell,r}| = \left| \sum_n C(n) \psi_N(n) \Phi_1(n) \overline{\Phi_2(n)} \right| \leq (q_0, \ell) \max_{t \in \mathbb{Z}/q_0\mathbb{Z}} \left| \sum_{n=t \pmod{q_0}} \psi_N(n) \Phi_1(n) \overline{\Phi_2(n)} \right|,$$

and by the second part of Corollary 4.16, we derive

$$|S_{\ell,r}| \ll (q_0, \ell) \left(\frac{[d_1, d_2]^{1/2}}{q_0^{1/2}} + \frac{N}{q_0} \frac{(c_1, \delta'_1)}{\delta'_1} \frac{(c_2, \delta'_2)}{\delta'_2} \right) \ll (q_0, \ell) \left(R^{1/2} \left(\frac{Q}{q_0} \right)^2 + \frac{N}{q_0} \frac{(c_1, \delta'_1)}{\delta'_1} \right)$$

where $\delta_i = d_i/(d_1, d_2)$ and $\delta'_i = \delta_i/(q_0, \delta_i)$, since

$$[d_1, d_2] \leq r q_0 q_1 q_2 s_1 s_2 \ll q_0 R \left(\frac{Q}{q_0} \right)^4, \quad \frac{(c_2, \delta'_2)}{\delta'_2} \leq 1.$$

Finally, we have

$$\frac{(c_1, \delta'_1)}{\delta'_1} = \prod_{\substack{p | \delta_1 \\ p \nmid c_1, q_0}} p \leq \frac{(c_1, r)}{r}$$

(since $r \mid \delta_1$ and $(r, q_0) = 1$). But a prime $p \mid r$ divides c_1 precisely when the r -component of (5.37) is constant, which happens exactly when $p \mid h_1 s_1 s_2 - h_2 q_1 q_2$, so that

$$S_{\ell,r} \ll (q_0, \ell) R^{1/2} \left(\frac{Q}{q_0} \right)^2 + \frac{(q_0, \ell) N}{q_0 R} (r, h_1 s_1 s_2 - h_2 q_1 q_2).$$

□

Remark 5.11. By replacing the lower bound $N \gg x^{1/2-2\varpi-c}$ with the lower bound $N \gg x^{1/2-\sigma}$, the above argument also yields the estimate $\text{Type}_I^{(1)}[\varpi, \delta, \sigma]$ whenever $48\varpi + 14\delta + 10\sigma < 1$. However, as this constraint does not allow σ to exceed $1/10$, one cannot use this estimate as a substitute for Theorem 2.8(ii) or Theorem 2.8(iii). If one uses the first estimate of Corollary 4.16 in place of the second, one can instead obtain $\text{Type}_I^{(1)}[\varpi, \delta, \sigma]$ for the range $56\varpi + 16\delta + 6\sigma < 1$, which now does permit σ to exceed $1/10$, and thus gives some version of Zhang's theorem after combining with a Type III estimate. However, σ still does not exceed $1/6$, and so one cannot dispense with the Type III component of the argument entirely with this Type I estimate. By using a second application of q -van der Corput, though (i.e. using the $l = 3$ case of Proposition 4.12 rather than the $l = 2$ case), it is possible to raise σ above $1/6$, assuming sufficient amounts of dense divisibility; we leave the details to the interested reader. However, the Cauchy-Schwarz arguments used here are not as efficient in the Type I setting as the Cauchy-Schwarz arguments in the sections below, and so these estimates do not supersede their Type I counterparts.

5.5. Proof of first Type I estimate. We will establish Theorem 5.8(i), which is the easiest of the Type I estimates to prove. The strategy follows closely that of the previous section. The changes, roughly speaking, are that the Cauchy-Schwarz argument is slightly modified (so that only the q_2 variable is duplicated, rather than both q_1 and q_2) and that we use an exponential sum estimate based on the first part of Corollary 4.16 instead of the second.

As before, we will establish the bound (5.32) for each individual r . We abbreviate again $\Upsilon = \Upsilon_{\ell,r}(b_1, b_2; q_0)$ and denote

$$H = x^\varepsilon R Q^2 M^{-1} q_0^{-1}.$$

We begin with the formula (5.33) for Υ , move the q_1 and n sums outside, apply the Cauchy-Schwarz inequality (and insert a suitable smooth coefficient sequence $\psi_N(n)$ at scale N to the n sum), so that we get

$$|\Upsilon|^2 \leq \Upsilon_1 \Upsilon_2$$

with

$$\Upsilon_1 := \sum_{q_1 \asymp Q/q_0} \sum_n C(n) |\beta(n)|^2 |\beta(n + \ell r)|^2 \ll \frac{NQ(q_0, \ell)}{q_0^2},$$

(as in (5.34)) and

$$\begin{aligned} \Upsilon_2 &:= \sum_n \psi_N(n) C(n) \sum_{q_1 \asymp Q/q_0} \left| \sum_{\substack{q_2 \asymp Q/q_0 \\ (q_1, q_2)=1}} \sum_{1 \leq |h| \leq H} c_{h, q_1, q_2} \Phi_\ell(h, n, r, q_0, q_1, q_2) \right|^2 \\ &= \sum_{q_1 \asymp Q/q_0} \sum_{\substack{q_2, s_2 \asymp Q/q_0 \\ (q_1, q_2)=(q_1, s_2)=1}} \sum_{1 \leq h_1, h_2 \leq |H|} c_{h_1, q_1, q_2} \overline{c_{h_2, q_1, s_2}} S_{\ell, r}(h_1, h_2, q_1, q_2, q_1, s_2), \end{aligned}$$

where $S_{\ell, r}$ is the same sum (5.35) as before and the variables (q_1, q_2, s_2) are restricted by the condition $q_0 q_1 r, q_0 q_2 r, q_0 s_2 r \in \mathcal{D}_I(x^\delta)$ (recall the definition (5.28)).

We will prove the following bound:

Proposition 5.12. *For any*

$$\mathbf{p} = (h_1, h_2, q_1, q_2, q_1, s_2)$$

with $(q_0 q_1 q_2 s_2, r) = 1$ and for any $\ell \neq 0$ and r as above with

$$\begin{aligned} q_0 q_i r, q_0 s_2 r &\in \mathcal{D}_I(x^\delta) \\ q_0 q_i &\ll Q, \quad q_0 s_2 \ll Q, \quad r \ll R, \end{aligned}$$

we have

$$|S_{\ell, r}(\mathbf{p})| \ll q_0^{1/6} N^{1/2} x^{\delta/6} (Q^3 R)^{1/6} + R^{-1} N (h_1 s_2 - h_2 q_2, r).$$

We first conclude assuming this estimate: arguing as in the previous section to sum the gcd $(h_1 s_2 - h_2 q_2, r)$, we obtain

$$\Upsilon_2 \ll \left(\frac{Q}{q_0}\right)^3 H^2 \left\{ q_0^{1/6} N^{1/2} (Q^3 R)^{1/6} x^{\delta/6} + \frac{N}{R} \right\} + H N \left(\frac{Q}{q_0}\right)^2,$$

and therefore

$$\begin{aligned} |\Upsilon|^2 &\ll \frac{NQ(q_0, \ell)}{q_0^2} \left\{ q_0^{1/6} \left(\frac{Q}{q_0}\right)^3 H^2 N^{1/2} (Q^3 R)^{1/6} x^{\delta/6} + \left(\frac{Q}{q_0}\right)^3 \frac{H^2 N}{R} + H N \left(\frac{Q}{q_0}\right)^2 \right\} \\ &\ll \frac{N^2 Q^4(q_0, \ell)^2}{q_0^4} \left\{ \frac{H^2 Q^{1/2} R^{1/6} x^{\delta/6}}{N^{1/2}} + \frac{H^2}{R} + \frac{H}{Q} \right\} \end{aligned}$$

where we once again discard some powers of $q_0 \geq 1$ from the denominator. Using again (5.13) and (5.14) and $N \ll M$, we find that

$$\begin{aligned} \frac{H^2 Q^{1/2} R^{1/6} x^{\delta/6}}{N^{1/2}} &\ll x^{\delta/6+2\varepsilon} \frac{R^{13/6} Q^{9/2}}{M^2 N^{1/2}} \ll x^{-2+\delta/6+2\varepsilon} \frac{N^{3/2} (QR)^{9/2}}{R^{7/3}} \ll \frac{x^{1/4+9\varpi+5\delta/2+9\varepsilon}}{N^{5/6}} \\ &\frac{H^2}{R} \ll \frac{x^{8\varpi+3\delta+11\varepsilon}}{N} \\ \frac{H}{Q} &\leq x^\varepsilon \frac{RQ}{M} \ll \frac{x^{1/2+2\varpi+\varepsilon}}{M} \ll x^{-c+\varepsilon}, \end{aligned}$$

and using the assumption $N \gg x^{1/2-\sigma}$ from (5.2), we will derive (5.32) if $c = 3\varepsilon$, $\varepsilon > 0$ is small enough, and

$$\begin{cases} \frac{1}{4} + 9\varpi + 5\frac{\delta}{2} < \frac{5}{6} \left(\frac{1}{2} - \sigma \right) \\ 8\varpi + 3\delta < \frac{1}{2} - \sigma \end{cases} \quad \Leftrightarrow \quad \begin{cases} 54\varpi + 15\delta + 5\sigma < 1 \\ 16\varpi + 6\delta + 2\sigma < 1. \end{cases}$$

For $\varpi, \delta, \sigma > 0$, the first condition implies the second (as its coefficients are larger). Since the first condition is the assumption of Theorem 5.8(i), we are then done.

We now prove the exponential sum estimate.

Proof of Proposition 5.12. We denote

$$\Phi_1(n) = \Phi_\ell(h_1, n, r, q_0, q_1, q_2), \quad \Phi_2(n) = \Phi_\ell(h_2, n, r, q_0, q_1, s_2),$$

as in the proof of Proposition 5.10, and we write

$$\Phi_1(n) \overline{\Phi_2(n)} = e_{d_1}^{(4)} \left(\frac{c_1}{n} \right) e_{d_2}^{(5)} \left(\frac{c_2}{n + \tau} \right)$$

for some c_1 and c_2 , where

$$d_1 := rq_0q_1, \quad d_2 := [q_2, s_2].$$

Since rq_0q_1 , rq_0q_2 and rq_0s_2 are x^δ -densely divisible, Lemma 2.10(ii) implies that the $\text{lcm}[d_1, d_2] = [rq_0q_1, rq_0q_2, rq_0s_2]$ is also x^δ -densely divisible.

Splitting again the factor $C(n)$ into residue classes modulo q_0 , and applying the first part of Corollary 4.16 to each residue class, we obtain

$$|S_{\ell,r}| \ll (q_0, \ell) \left(\frac{N^{1/2}}{q_0^{1/2}} [d_1, d_2]^{1/6} x^{\delta/6} + \frac{N}{q_0} \frac{(c_1, \delta'_1)}{\delta_1} \frac{(c_2, \delta'_2)}{\delta'_2} \right)$$

where $\delta_i = d_i/(d_1, d_2)$ and $\delta'_i = \delta_i/(q_0, \delta_i)$. Again, as in the proof of Proposition 5.10, we conclude by observing that $[d_1, d_2] \leq Q^3 R/q_0$, $(c_2, \delta'_2)/\delta'_2 \leq 1$ while

$$\frac{(c_1, \delta'_1)}{\delta'_1} \leq \frac{(c_1, r)}{r},$$

and inspection of the r -component of $\Phi_1(n) \overline{\Phi_2(n)}$ using (5.29) shows that a prime $p \mid r$ divides c_1 if and only if $p \mid h_1 s_2 - h_2 q_2$. \square

5.6. Proof of second Type I estimate. We finish this section with the proof of Theorem 5.8(ii). The idea is very similar to the previous Type I estimate, the main difference being that since q_1 (and q_2) is densely divisible in this case, we can split the sum over q_1 to obtain a better balance of the factors in the Cauchy-Schwarz inequality.

As before, we will prove the bound (5.32) for individual r , and we abbreviate $\Upsilon = \Upsilon_{\ell,r}(b_1, b_2; q_0)$ and denote

$$H = x^\varepsilon R Q^2 M^{-1} q_0^{-1}.$$

We may assume that $H \geq 1$, since otherwise the bound is trivial. We note that $q_0 q_1$ is, by assumption, $x^{\delta+o(1)}$ -densely divisible, and therefore by Lemma 2.10(i), q_1 is y -densely divisible with $y = q_0 x^{\delta+o(1)}$. Furthermore we have

$$x^{-2\varepsilon} Q/H \gg x^{c-3\varepsilon}$$

by (5.13) and $M \gg x^{1/2+2\varpi+c}$, and

$$x^{-2\varepsilon} Q/H \ll q_1 y = q_1 q_0 x^{\delta+o(1)}$$

since $q_1 q_0 \asymp Q$ and $H \geq 1$. Thus (assuming $c > 3\varepsilon$) we can factor

$$q_1 = u_1 v_1$$

where u_1, v_1 are squarefree with

$$\begin{aligned} q_0^{-1} x^{-\delta-2\varepsilon} Q/H &\ll u_1 \ll x^{-2\varepsilon} Q/H \\ q_0^{-1} x^{2\varepsilon} H &\ll v_1 \ll x^{\delta+2\varepsilon} H \end{aligned}$$

(either from dense divisibility if $x^{-2\varepsilon} Q/H \ll q_1$, or taking $u_1 = q_1, v_1 = 1$ otherwise).

Let

$$\Upsilon_{U,V} := \sum_{1 \leq |h| \leq H} \sum_{u_1 \asymp U} \sum_{v_1 \asymp V} \sum_{\substack{q_2 \asymp Q/q_0 \\ (u_1 v_1, q_0 q_2) = 1}} \left| \sum_n C(n) \beta(n) \overline{\beta(n + \ell r)} \Phi_\ell(h, n, r, q_0, u_1 v_1, q_2) \right|,$$

where u_1, v_1 are understood to be squarefree.

By dyadic decomposition of the sum over $q_1 = u_1 v_1$ in Υ , it is enough to prove that

$$\Upsilon_{U,V} \ll x^{-\varepsilon}(q_0, \ell) Q^2 N q_0^{-2} \quad (5.38)$$

whenever

$$q_0^{-1} x^{-\delta-2\varepsilon} Q/H \ll U \ll x^{-2\varepsilon} Q/H \quad (5.39)$$

$$q_0^{-1} x^{2\varepsilon} H \ll V \ll x^{\delta+2\varepsilon} H \quad (5.40)$$

$$UV \asymp Q/q_0. \quad (5.41)$$

We replace the modulus by complex numbers c_{h,u_1,v_1,q_2} of modulus at most 1, move the sum over n, u_1 and q_2 outside and apply the Cauchy-Schwarz inequality as in the previous sections to obtain

$$|\Upsilon_{U,V}|^2 \leq \Upsilon_1 \Upsilon_2$$

with

$$\Upsilon_1 := \sum_{\substack{u_1 \asymp U \\ q_2 \asymp Q/q_0}} \sum_n C(n) |\beta(n)|^2 |\beta(n + \ell r)|^2 \ll (q_0, \ell) \frac{N Q U}{q_0^2}$$

as in (5.34) and

$$\begin{aligned} \Upsilon_2 &:= \sum_{\substack{u_1 \asymp U \\ q_2 \asymp Q/q_0}} \sum_n \psi_N(n) C(n) \left| \sum_{v_1 \asymp V; (u_1 v_1, q_0 q_2)=1} \sum_{1 \leq |h| \leq H} c_{h, u_1, v_1, q_2} \Phi_\ell(h, n, r, q_0, u_1 v_1, q_2) \right|^2 \\ &= \sum_{\substack{u_1 \asymp U \\ q_2 \asymp Q/q_0}} \sum_{v_1, v_2 \asymp V; (u_1 v_1 v_2, q_0 q_2)=1} \sum_{1 \leq |h_1|, |h_2| \leq H} c_{h_1, u_1, v_1, q_2} \overline{c_{h_2, u_1, v_2, q_2}} T_{\ell, r}(h_1, h_2, u_1, v_1, v_2, q_2, q_0) \end{aligned}$$

where the exponential sum $T_{\ell, r}$ is a variant of $S_{\ell, r}$ given by

$$T_{\ell, r} := \sum_n C(n) \psi_N(n) \Phi_\ell(h_1, n, r, q_0, u_1 v_1, q_2) \overline{\Phi_\ell(h_2, n, r, q_0, u_1 v_2, q_2)}. \quad (5.42)$$

The analogue of Propositions 5.10 and 5.12 is:

Proposition 5.13. *For any*

$$\mathbf{p} = (h_1, h_2, u_1, v_1, v_2, q_2, q_0)$$

with $(u_1 v_1 v_2, q_0 q_2) = (q_0, q_2) = 1$, any $\ell \neq 0$ and r as above, we have

$$|T_{\ell, r}(\mathbf{p})| \ll (q_0, \ell) \left(q_0^{-1/2} N^{1/2} x^{\delta/3 + \varepsilon/3} (RHQ^2)^{1/6} + \frac{N}{q_0 R} (h_1 v_2 - h_2 v_1, r) \right).$$

Assuming this, we derive as before

$$\Upsilon_2 \ll (q_0, \ell) H^2 UV^2 \left(\frac{Q}{q_0} \right) \left\{ N^{1/2} (RHQ^2)^{1/6} x^{\delta/3 + \varepsilon/3} + \frac{N}{R} \right\} + HNUV \left(\frac{Q}{q_0} \right),$$

and then

$$\begin{aligned} |\Upsilon_{U, V}|^2 &\ll (q_0, \ell)^2 \frac{NQU}{q_0} \left\{ \frac{H^2 Q^3 N^{1/2} (HQ^2 R)^{1/6} x^{\delta/3 + \varepsilon/3}}{U q_0^3} + \frac{H^2 N Q^3}{U R q_0^3} + H N \left(\frac{Q^2}{q_0^3} \right) \right\} \\ &\ll (q_0, \ell)^2 \frac{N^2 Q^4}{q_0^4} \left\{ \frac{H^{13/6} Q^{1/3} R^{1/6} x^{\delta/3 + \varepsilon/3}}{N^{1/2}} + \frac{H^2}{R} + \frac{H}{V q_0} \right\} \end{aligned}$$

since $UV \asymp Q/q_0$, where we have again discarded a factor of q_0 in the first line. Using again (5.13), (5.14), (5.40), we find that

$$\begin{aligned} \frac{H^{13/6} Q^{1/3} R^{1/6} x^{\delta/3 + \varepsilon/3}}{N^{1/2}} &\ll x^{\delta + 5\varepsilon/2} \frac{R^{7/3} Q^{14/3}}{N^{1/2} M^{13/6}} \ll x^{1/6 + 28\varpi/3 + \delta/3 + 5\varepsilon/2} \frac{N^{5/3}}{R^{7/3}} \\ &\ll \frac{x^{28\varpi/3 + 8\delta/3 + 1/6 + 19\varepsilon/2}}{N^{2/3}} \\ \frac{H^2}{R} &\ll \frac{x^{8\varpi + 3\delta + 11\varepsilon}}{N} \\ \frac{H}{V q_0} &\ll x^{-2\varepsilon}, \end{aligned}$$

and therefore (5.38) holds for sufficiently small ε provided

$$\begin{cases} \frac{28\varpi}{3} + \frac{8\delta}{3} + \frac{1}{6} < \frac{2}{3} \left(\frac{1}{2} - \sigma \right) \\ 8\varpi + 3\delta < \frac{1}{2} - \sigma \end{cases} \Leftrightarrow \begin{cases} 56\varpi + 16\delta + 4\sigma < 1 \\ 16\varpi + 6\delta + 2\sigma < 1. \end{cases}$$

Again the first condition implies the second, and the proof is completed.

Proof of Proposition 5.13. We proceed as in the previous cases. Denoting

$$\Phi_1(n) := \Phi_\ell(h_1, n, r, q_0, u_1 v_1, q_2), \quad \Phi_2(n) := \Phi_\ell(h_2, n, r, q_0, u_1 v_2, q_2)$$

for brevity, we may write

$$\Phi_1(n) \overline{\Phi_2(n)} = e_{d_1}^{(4)} \left(\frac{c_1}{n} \right) e_{d_2}^{(5)} \left(\frac{c_2}{n + \tau} \right)$$

by (5.29) for some c_1 and c_2 and τ , where

$$d_1 := r q_0 u_1 [v_1, v_2], \quad d_2 := q_2.$$

Since $r q_0 u_1 v_1$, $r q_0 u_1 v_2$ and $r q_0 q_2$ are x^δ -densely divisible, Lemma 2.10(ii) implies that their gcd $[d_1, d_2]$ is also x^δ -densely divisible.

Splitting again the factor $C(n)$ into residue classes modulo q_0 , and applying the first part of Corollary 4.16 to each residue class, we obtain

$$|T_{\ell, r}| \ll (q_0, \ell) \left(\frac{N^{1/2}}{q_0^{1/2}} [d_1, d_2]^{1/6} x^{\delta/6} + \frac{N}{q_0} \frac{(c_1, \delta'_1)}{\delta'_1} \frac{(c_2, \delta'_2)}{\delta'_2} \right)$$

where $\delta_i = d_i / (d_1, d_2)$ and $\delta'_i = \delta_i / (q_0, \delta_i)$. We conclude as before by observing that

$$[d_1, d_2] \ll QRUV^2 \ll x^{\delta+2\varepsilon} \frac{H Q^2 R}{q_0},$$

by (5.40) and (5.41), that $(c_2, \delta_2) / \delta_2 \leq 1$ and that $(c_1, \delta) / \delta_1 \leq (c_1, r) / r$, where inspection of the r -component of $\Phi_1(n) \overline{\Phi_2(n)}$ using (5.29) shows that a prime $p \mid r$ divides c_1 if and only if $p \mid h_1 v_2 - h_2 v_1$. \square

6. TRACE FUNCTIONS AND MULTIDIMENSIONAL EXPONENTIAL SUM ESTIMATES

In this section (as in Section 4), we do not use the standard asymptotic convention (Definition 1.2), since we discuss general ideas that are of interest independently of the goal of bounding gaps between primes.

We will discuss some of the machinery and formalism of ℓ -adic sheaves \mathcal{F} on curves⁵ and their associated *Frobenius trace functions* $t_{\mathcal{F}}$. This will allow us to state and then apply the deep theorems of Deligne's general form of the Riemann Hypothesis over finite fields for such sheaves. We will use these theorems to establish certain estimates for multi-variable exponential sums which go beyond the one-dimensional estimates obtainable from Lemma 4.2 (specifically, the estimates we need are stated in Corollary 6.24 and Corollary 6.26).

The point is that these Frobenius trace functions significantly generalize the rational phase functions $x \mapsto e_p \left(\frac{P(x)}{Q(x)} \right)$ which appear in Lemma 4.2. They include more general functions, such as the hyper-Kloosterman sums

$$x \mapsto \frac{(-1)^{m-1}}{p^{\frac{m-1}{2}}} \sum_{\substack{y_1, \dots, y_m \in \mathbb{F}_p \\ y_1 \dots y_m = x}} \dots \sum e_p(y_1 + \dots + y_m),$$

and satisfy a very flexible formalism. In particular, the class of Frobenius trace functions is (essentially) closed under basic operations such as pointwise addition and multiplication, complex conjugation, change of variable (pullback), and the normalized Fourier

⁵In our applications, the only curves U we deal with are obtained by removing a finite number of points from the projective line \mathbb{P}^1 .

transform. Using these closure properties allows us to build a rich class of useful trace functions from just a small set of basic trace functions. In fact, the sheaves we actually use in this paper are ultimately obtained from only two sheaves: the Artin-Schreier sheaf and the third hyper-Kloosterman sheaf.⁶ However, we have chosen to discuss more general sheaves in this section in order to present the sheaf-theoretic framework in a more natural fashion.

Because exponential sums depending on a parameter are often themselves trace functions, one can recast many multidimensional exponential sums (e.g.

$$\sum_{x_1, \dots, x_n \in \mathbb{F}_p} e_p(f(x_1, \dots, x_n))$$

for some rational function $f \in \mathbb{F}_p(X_1, \dots, X_n)$ in terms of one-dimensional sums of Frobenius trace functions. As a very rough first approximation, Deligne's results [9] imply that the square root cancellation exhibited in Lemma 4.2 is also present for these more general sums of Frobenius trace functions, as long as certain degenerate cases are avoided. Therefore, at least in principle, this implies square root cancellation for many multidimensional exponential sums.

In practice, this is often not entirely straightforward, as we will explain. One particular issue is that the bounds provided by Deligne's theorems depend on a certain measure of complexity of the ℓ -adic sheaf defining the trace function, which is known as the *conductor* of a sheaf. In estimates for sums of trace functions, this conductor plays the same role that the degrees of the polynomials f, g play in Lemma 4.2. We will therefore have to expend some effort to control the conductors of various sheaves before we can extract usable estimates from Deligne's results.

This section is not self-contained, and assumes a certain amount of prior formal knowledge of the terminology of ℓ -adic cohomology on curves. For readers who are not familiar with this material, we would recommend as references such surveys as [30, §11.11], [35], [20], and some of the books and papers of Katz, in particular [31, 33, 32], as well as Deligne's own account [7, Sommes trig.]. We would like to stress that, if the main results of the theory are assumed and the construction of some main objects (e.g. the Artin-Schreier and hyper-Kloosterman sheaves) is accepted, working with ℓ -adic sheaves essentially amounts to studying certain finite-dimensional continuous representations of the Galois group of the field $\mathbb{F}_p(X)$ of rational functions over \mathbb{F}_p .

Alternatively, for the purposes of establishing only the bounds on (incomplete) multi-variable exponential sums used in the proofs of the main theorems of this paper (namely the bounds in Corollary 6.24 and Corollary 6.26), it is possible to ignore all references to sheaves, if one accepts the estimates on complete multi-dimensional exponential sums in Proposition 6.11 and Theorem 6.17 as “black boxes”; the estimates on incomplete exponential sums will be deduced from these results via completion of sums and the q -van der Corput A -process.

6.1. ℓ -adic sheaves on the projective line. For p a prime, we fix an algebraic closure $\overline{\mathbb{F}_p}$ of \mathbb{F}_p and denote by $k \subset \overline{\mathbb{F}_p} = \overline{k}$ a finite extension of \mathbb{F}_p . Its cardinality is usually denoted $|k| = p^{[k:\mathbb{F}_p]} = p^{\deg(k)} = q$. For us, the Frobenius element relative to k means

⁶One can even reduce the number of generating sheaves to one, because the sheaf-theoretic Fourier transform, combined with pullback via the inversion map $x \mapsto \frac{1}{x}$, may be used to iteratively build the hyper-Kloosterman sheaves from the Artin-Schreier sheaf.

systematically the *geometric Frobenius* Fr_k , which is the inverse in $\text{Gal}(\bar{k}/k)$ of the *arithmetic Frobenius*, $x \mapsto x^q$ on \bar{k} .

We denote by $K = \mathbb{F}_p(t)$ the function field of the projective line $\mathbb{P}_{\mathbb{F}_p}^1$ and by $\bar{K} \supset \bar{\mathbb{F}_p}$ some separable closure; let $\bar{\eta} = \text{Spec}(\bar{K})$ be the corresponding geometric generic point.

We fix another prime $\ell \neq p$, and we denote by $\iota: \bar{\mathbb{Q}_\ell} \hookrightarrow \mathbb{C}$ an algebraic closure of the field \mathbb{Q}_ℓ of ℓ -adic numbers, together with an embedding into the complex numbers. By an ℓ -adic sheaf \mathcal{F} on a noetherian scheme X (in practice, a curve), we always mean a constructible sheaf of finite-dimensional $\bar{\mathbb{Q}_\ell}$ -vector spaces with respect to the étale topology on X , and we recall that the category of ℓ -adic sheaves is abelian.

We will be especially interested in the case $X = \mathbb{P}_k^1$ (the projective line) and we will use the following notation for the translation, dilation, and fractional linear maps from \mathbb{P}^1 to itself:

$$\begin{aligned} [+l]: x &\mapsto x + l, \\ [\times a]: x &\mapsto ax, \\ \gamma: x &\mapsto \gamma \cdot x = \frac{ax + b}{cx + d} \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_p). \end{aligned}$$

We will often transform a sheaf \mathcal{F} on \mathbb{P}_k^1 by applying pullback by one of the above maps, and we denote these pullback sheaves by $[+l]^*\mathcal{F}$, $[\times a]^*\mathcal{F}$ and $\gamma^*\mathcal{F}$.

6.1.1. Galois representations. The category of ℓ -adic sheaves on \mathbb{P}_k^1 admits a relatively concrete description in terms of representations of the Galois group $\text{Gal}(\bar{K}/k.K)$. We recall some important features of it here and we refer to [31, 4.4] for a complete presentation.

For $j: U \hookrightarrow \mathbb{P}_k^1$ some non-empty open subset defined over k , we denote by $\pi_1(U)$ (resp. $\pi_1^g(U)$) the *arithmetic* (resp. *geometric*) *fundamental group* of U , which may be defined as the quotient of $\text{Gal}(\bar{K}/k.K)$ (resp. of $\text{Gal}(\bar{K}/\bar{k}.K)$) by the smallest closed normal subgroup containing all the inertia subgroups above the closed points of U . We have then a commutative diagram of short exact sequences of groups

$$\begin{array}{ccccccc} 1 & \longrightarrow & \text{Gal}(\bar{K}/\bar{k}.K) & \longrightarrow & \text{Gal}(\bar{K}/k.K) & \longrightarrow & \text{Gal}(\bar{k}/k) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow = \\ 1 & \longrightarrow & \pi_1^g(U) & \longrightarrow & \pi_1(U) & \longrightarrow & \text{Gal}(\bar{k}/k) \longrightarrow 1 \end{array} \quad (6.1)$$

Given an ℓ -adic sheaf \mathcal{F} on \mathbb{P}_k^1 , there exists some non-empty (hence dense, in the Zariski topology) open set $j: U \hookrightarrow \mathbb{P}_k^1$ such that the pullback $j^*\mathcal{F}$ (the restriction of \mathcal{F} to U) is *lisse*, or in other words, for which $j^*\mathcal{F}$ “is” a finite-dimensional continuous representation $\rho_{\mathcal{F}}$ of $\text{Gal}(\bar{K}/k.K)$ factoring through $\pi_1(U)$

$$\rho_{\mathcal{F}}: \text{Gal}(\bar{K}/k.K) \twoheadrightarrow \pi_1(U) \rightarrow \text{GL}(\mathcal{F}_{\bar{\eta}}),$$

where the geometric generic stalk $\mathcal{F}_{\bar{\eta}}$ of \mathcal{F} is a finite-dimensional $\bar{\mathbb{Q}_\ell}$ -vector space. Its dimension is the (*generic*) *rank* of \mathcal{F} and is denoted $\text{rk}(\mathcal{F})$. There is a maximal (with respect to inclusion) open subset on which \mathcal{F} is lisse, which will be denoted $U_{\mathcal{F}}$.

We will freely apply the terminology of representations to ℓ -adic sheaves. The properties of $\rho_{\mathcal{F}}$ as a representation of the arithmetic Galois group $\text{Gal}(\bar{K}/k.K)$ (or of the

arithmetic fundamental group $\pi_1(U)$) will be qualified as “arithmetic”, while the properties of its restriction $\rho_{\mathcal{F}}^g$ to the geometric Galois group $\text{Gal}(\overline{K}/k.K)$ (or the geometric fundamental group $\pi_1^g(U)$) will be qualified as “geometric”. For instance, we will say that \mathcal{F} is *arithmetically irreducible* (resp. *geometrically irreducible*) or *arithmetically isotypic* (resp. *geometrically isotypic*) if the corresponding arithmetic representation $\rho_{\mathcal{F}}$ (resp. the geometric representation $\rho_{\mathcal{F}}^g$) is.

We will be mostly interested in the geometric properties of a sheaf, therefore we will usually omit the adjective “geometric” in our statements, so that “isotypic” will mean “geometrically isotypic”. We will always spell out explicitly when an arithmetic property is intended, so that no confusion can arise.

6.1.2. Middle-extension sheaves. An ℓ -adic sheaf is called a *middle-extension* sheaf if, for some (and in fact, for any) non-empty open subset $j : U \hookrightarrow \mathbb{P}_k^1$ such that $j^*\mathcal{F}$ is lisse, we have an arithmetic isomorphism

$$\mathcal{F} \simeq j_*j^*\mathcal{F},$$

or equivalently if, for every $\bar{x} \in \mathbb{P}^1(\bar{k})$, the specialization maps (cf. [31, 4.4])

$$s_{\bar{x}} : \mathcal{F}_{\bar{x}} \rightarrow \mathcal{F}_{\bar{\eta}}^{I_{\bar{x}}}$$

are isomorphisms, where $I_{\bar{x}}$ is the inertia subgroup at \bar{x} . Given an ℓ -adic sheaf, its associated middle-extension is the sheaf

$$\mathcal{F}^{\text{me}} = j_*j^*\mathcal{F}$$

for some non-empty open subset $j : U \hookrightarrow \mathbb{P}_k^1$ on which \mathcal{F} is lisse. This sheaf is a middle-extension sheaf, and is (up to arithmetic isomorphism) the unique middle-extension sheaf whose restriction to U is arithmetically isomorphic to that of \mathcal{F} . In particular, \mathcal{F}^{me} does not depend on the choice of U .

6.2. The trace function of a sheaf. Let \mathcal{F} be an ℓ -adic sheaf on the projective line over \mathbb{F}_p . For each finite extension k/\mathbb{F}_p , \mathcal{F} defines a complex valued function

$$x \mapsto t_{\mathcal{F}}(x; k)$$

on $k \cup \{\infty\} = \mathbb{P}^1(k)$, which is called the *Frobenius trace function*, or just *trace function*, associated with \mathcal{F} and k . It is defined by

$$\mathbb{P}^1(k) \ni x \mapsto t_{\mathcal{F}}(x; k) := \iota(\text{Tr}(\text{Fr}_{x,k}|\mathcal{F}_{\bar{x}})).$$

Here $\bar{x} : \text{Spec}(\bar{k}) \rightarrow \mathbb{P}_k^1$ denotes a geometric point above x , and $\mathcal{F}_{\bar{x}}$ is the stalk of \mathcal{F} at that point, which is a finite-dimensional $\overline{\mathbb{Q}}_{\ell}$ -vector space on which $\text{Gal}(\bar{k}/k)$ acts linearly, and $\text{Fr}_{x,k}$ denotes the geometric Frobenius of that Galois group. The trace of the action of this operator is independent of the choice of \bar{x} .

If $k = \mathbb{F}_p$, which is the case of importance for the applications in this paper, we will write $t_{\mathcal{F}}(x; p)$ or simply $t_{\mathcal{F}}(x)$ instead of $t_{\mathcal{F}}(x; \mathbb{F}_p)$.

If $x \in U_{\mathcal{F}}(k)$, the quantity $t_{\mathcal{F}}(x; k)$ is simply the trace of the geometric Frobenius conjugacy class of a place of \overline{K} above x acting through the associated representation $\mathcal{F}_{\bar{\eta}}$, i.e., the value (under ι) of the character of the representation at this conjugacy class:

$$t_{\mathcal{F}}(x; k) = \iota(\text{Tr}(\text{Fr}_{x,k}|\mathcal{F}_{\bar{\eta}})).$$

If \mathcal{F} is a middle-extension sheaf one has more generally

$$t_{\mathcal{F}}(x; k) = \iota(\text{Tr}(\text{Fr}_{x,k}|\mathcal{F}_{\bar{\eta}}^{I_{\bar{x}}}).$$

For any sheaf \mathcal{F} , the trace function of \mathcal{F} restricted to $U_{\mathcal{F}}(k)$ coincides with the restriction of the trace function of \mathcal{F}^{me} .

6.2.1. *Purity and admissibility.* The following notion was introduced by Deligne [9].

Definition 6.1 (Purity). For $i \in \mathbb{Z}$, an ℓ -adic sheaf on $\mathbb{P}_{\mathbb{F}_p}^1$ is *generically pure* (or *pure*, for short) of weight i if, for any k/\mathbb{F}_p and any $x \in U_{\mathcal{F}}(k)$, the eigenvalues of $\text{Fr}_{x,k}$ acting on $\mathcal{F}_{\bar{\eta}}$ are \mathbb{Q} -algebraic numbers whose Galois conjugates have complex absolute value equal to $q^{i/2} = |k|^{i/2}$.

Remark 6.2. Deligne proved (see [9, (1.8.9)]) that if \mathcal{F} is generically pure of weight i , then for any k/\mathbb{F}_p and any $x \in \mathbb{P}^1(k)$, the eigenvalues of $\text{Fr}_{x,k}$ acting on $\mathcal{F}_{\bar{\eta}}^{I_{\bar{x}}}$ are \mathbb{Q} -algebraic numbers whose Galois conjugates have complex absolute value $\leq q^{i/2}$.

In particular, if \mathcal{F} is a middle-extension sheaf which is pointwise pure of weight i , then we get

$$|t_{\mathcal{F}}(x; k)| = |\iota(\text{Tr}(\text{Fr}_x | \mathcal{F}_{\bar{\eta}}^{I_{\bar{x}}}))| \leq \text{rk}(\mathcal{F}) q^{i/2} \quad (6.2)$$

for any $x \in \mathbb{P}^1(k)$.

We can now describe the class of sheaves and trace functions that we will work with.

Definition 6.3 (Admissible sheaves). Let k be a finite extension of \mathbb{F}_p . An *admissible sheaf* over k is a middle-extension sheaf on \mathbb{P}_k^1 which is pointwise pure of weight 0. An *admissible trace function* over k is a function $k \rightarrow \mathbb{C}$ which is equal to the trace function of some admissible sheaf restricted to $k \subset \mathbb{P}^1(k)$.

Remark 6.4. The weight 0 condition may be viewed as a normalization to ensure that admissible trace functions typically have magnitude comparable to 1. Sheaves which are pure of some other weight can be studied by reducing to the 0 case by the simple device of *Tate twists*. However, we will not need to do this, as we will be working exclusively with sheaves which are pure of weight 0.

6.2.2. *Conductor.* Let \mathcal{F} be a middle-extension sheaf on \mathbb{P}_k^1 . The *conductor* of \mathcal{F} is defined to be

$$\text{cond}(\mathcal{F}) := \text{rk}(\mathcal{F}) + |(\mathbb{P}^1 - U_{\mathcal{F}})(\bar{k})| + \sum_{x \in (\mathbb{P}^1 - U_{\mathcal{F}})(\bar{k})} \text{swan}_x(\mathcal{F})$$

where $\text{swan}_x(\mathcal{F})$ denotes the Swan conductor of the representation $\rho_{\mathcal{F}}$ at x , a non-negative integer measuring the “wild ramification” of $\rho_{\mathcal{F}}$ at x (see e.g. [32, Definition 1.6] for the precise definition of the Swan conductor). If $\text{swan}_x(\mathcal{F}) = 0$, one says that \mathcal{F} is *tamely ramified* at x , and otherwise that it is *wildly ramified*.

The invariant $\text{cond}(\mathcal{F})$ is a non-negative integer (positive if $\mathcal{F} \neq 0$) and it measures the complexity of the sheaf \mathcal{F} and of its trace function $t_{\mathcal{F}}$. For instance, if \mathcal{F} is admissible, so that it is also pure of weight 0, then we deduce from (6.2) that

$$|t_{\mathcal{F}}(x; k)| \leq \text{rk}(\mathcal{F}) \leq \text{cond}(\mathcal{F}) \quad (6.3)$$

for any $x \in k$.

6.2.3. Dual and Tensor Product. Given admissible sheaves \mathcal{F} and \mathcal{G} on \mathbb{P}_k^1 , their tensor product, denoted $\mathcal{F} \otimes \mathcal{G}$, is by definition the middle-extension sheaf associated to the tensor product representation $\rho_{\mathcal{F}} \otimes \rho_{\mathcal{G}}$ (computed over the intersection of $U_{\mathcal{F}}$ and $U_{\mathcal{G}}$, which is still a dense open set of \mathbb{P}_k^1). Note that this sheaf may be different from the tensor product of \mathcal{F} and \mathcal{G} as constructible sheaves (similarly to the fact that the product of two primitive Dirichlet characters is not necessarily primitive).

Similarly, the dual of \mathcal{F} , denoted $\check{\mathcal{F}}$, is defined as the middle extension sheaf associated to the contragredient representation $\check{\rho}_{\mathcal{F}}$.

We have

$$U_{\mathcal{F}} \cap U_{\mathcal{G}} \subset U_{\mathcal{F} \otimes \mathcal{G}}, \quad U_{\check{\mathcal{F}}} = U_{\mathcal{F}}.$$

It is not obvious, but true, that the tensor product and the dual of admissible sheaves are admissible. We then have

$$t_{\mathcal{F} \otimes \mathcal{G}}(x; k) = t_{\mathcal{F}}(x; k) t_{\mathcal{G}}(x; k), \quad t_{\check{\mathcal{F}}}(x; k) = \overline{t_{\mathcal{F}}(x; k)} \quad (6.4)$$

for $x \in U_{\mathcal{F}}(k) \cap U_{\mathcal{G}}(k)$ and $x \in \mathbb{P}^1(k)$, respectively. In particular, the product of two admissible trace functions $t_{\mathcal{F}}$ and $t_{\mathcal{G}}$ coincides with an admissible trace function outside a set of at most $\text{cond}(\mathcal{F}) + \text{cond}(\mathcal{G})$ elements, and the complex conjugate of an admissible trace function is again an admissible trace function.

We also have

$$\text{cond}(\check{\mathcal{F}}) = \text{cond}(\mathcal{F}) \quad (6.5)$$

(which is easy to check from the definition of Swan conductors) and

$$\text{cond}(\mathcal{F} \otimes \mathcal{G}) \ll \text{rk}(\mathcal{F}) \text{rk}(\mathcal{G}) \text{cond}(\mathcal{F}) \text{cond}(\mathcal{G}) \leq \text{cond}(\mathcal{F})^2 \text{cond}(\mathcal{G})^2 \quad (6.6)$$

where the implied constant is absolute (which is also relatively elementary, see [15, Prop. 8.2(2)] or [19, Lemma 4.8]).

6.3. Irreducible components and isotypic decomposition. Let k be a finite field, let \mathcal{F} be an admissible sheaf over \mathbb{P}_k^1 and consider $U = U_{\mathcal{F}}$ and the corresponding open immersion $j: U \hookrightarrow \mathbb{P}_k^1$. A fundamental result of Deligne [9, (3.4.1)] proves that $\rho_{\mathcal{F}}$ is then geometrically semisimple. Thus there exist lisse sheaves \mathcal{G} on $U \times \bar{k}$, irreducible and pairwise non-isomorphic, and integers $n(\mathcal{G}) \geq 1$, such that we have

$$j^* \mathcal{F} \simeq \bigoplus_{\mathcal{G}} \mathcal{G}^{n(\mathcal{G})}$$

as an isomorphism of lisse sheaves on $U \times \bar{k}$ (the \mathcal{G} might not be defined over k). Extending with j_* to $\mathbb{P}_{\bar{k}}^1$ we obtain a decomposition

$$\mathcal{F} \simeq \bigoplus_{\mathcal{G}} j_* \mathcal{G}^{n(\mathcal{G})}$$

where each $j_* \mathcal{G}$ is a middle-extension sheaf over \bar{k} . We call the sheaves $j_* \mathcal{G}$ the *geometrically irreducible components* of \mathcal{F} .

Over the open set $U_{\mathcal{F}}$, we can define the arithmetic semisimplification $\rho_{\mathcal{F}}^{\text{ss}}$ as the direct sum of the Jordan-Hölder arithmetically irreducible components of the representation $\rho_{\mathcal{F}}$. Each arithmetically irreducible component is either geometrically isotypic or induced from a proper finite index subgroup of $\pi_1(U_{\mathcal{F}})$. If an arithmetically irreducible component π is induced, it follows that the trace function of the middle-extension sheaf

corresponding to π vanishes identically. Thus, if we denote by $\text{Iso}(\mathcal{F})$ the set of middle-extensions associated to the geometrically isotypic components of $\rho_{\mathcal{F}}^{\text{ss}}$, we obtain an identity

$$t_{\mathcal{F}} = \sum_{\mathcal{G} \in \text{Iso}(\mathcal{F})} t_{\mathcal{G}} \quad (6.7)$$

(indeed, these two functions coincide on $U_{\mathcal{F}}$ and are both trace functions of middle-extension sheaves), where each summand is admissible. For these facts, we refer to [31, §4.4, §4.5] and [15, Prop. 8.3].

6.4. Deligne's main theorem and quasi-orthogonality. The generalizations of complete exponential sums over finite fields that we consider are sums

$$S(\mathcal{F}; k) = \sum_{x \in k} t_{\mathcal{F}}(x; k)$$

for any admissible sheaf \mathcal{F} over \mathbb{P}_k^1 . By (6.3), we have the trivial bound

$$|S(\mathcal{F}; k)| \leq \text{cond}(\mathcal{F})|k| = \text{cond}(\mathcal{F})q.$$

Deligne's main theorem [9, Thm. 1] provides strong non-trivial estimates for such sums, at least when p is large compared to $\text{cond}(\mathcal{F})$.

Theorem 6.5 (Sums of trace functions). *Let \mathcal{F} be an admissible sheaf on \mathbb{P}_k^1 where $|k| = q$ and $U = U_{\mathcal{F}}$. We have*

$$S(\mathcal{F}; k) = q \text{Tr}(\text{Fr}_k | (\mathcal{F}_{\bar{\eta}})_{\pi_1^q(U)}) + O(\text{cond}(\mathcal{F})^2 q^{1/2})$$

where $(\mathcal{F}_{\bar{\eta}})_{\pi_1^q(U)}$ denotes the Tate-twisted $\pi_1^q(U_{\mathcal{F}})$ -coinvariant space⁷ of $\rho_{\mathcal{F}}$, on which $\text{Gal}(\bar{k}/k)$ acts canonically, and where the implied constant is effective and absolute.

Proof. Using (6.3), we have

$$S(\mathcal{F}; k) = \sum_{x \in U(k)} t_{\mathcal{F}}(x; k) + O(\text{cond}(\mathcal{F})^2)$$

where the implied constant is at most 1. The Grothendieck-Lefschetz trace formula (see, e.g., [32, Chap. 3]) gives

$$S_{\mathcal{F}}(U, k) = \sum_{i=0}^2 (-1)^i \text{Tr}(\text{Fr}_k | H_c^i(U \otimes_k \bar{k}, \mathcal{F}))$$

where $H_c^i(U \otimes_k \bar{k}, \mathcal{F})$ is the i^{th} compactly supported étale cohomology group of the base change of U to \bar{k} with coefficients in \mathcal{F} , on which the global Frobenius automorphism Fr_k acts.

Since U is affine and \mathcal{F} is lisse on U , it is known that $H_c^0(U \otimes_k \bar{k}, \mathcal{F}) = 0$. For $i = 1$, Deligne's main theorem shows that, because \mathcal{F} is of weight 0, all eigenvalues of Fr_k acting on $H_c^1(U \otimes_k \bar{k}, \mathcal{F})$ are algebraic numbers with complex absolute value $\leq |k|^{1/2}$, so that

$$|\text{Tr}(\text{Fr}_k | H_c^1(U \otimes_k \bar{k}, \mathcal{F}))| \leq \dim(H_c^1(U \otimes_k \bar{k}, \mathcal{F})) q^{1/2}.$$

Using the Euler-Poincaré formula and the definition of the conductor, one easily obtains

$$\dim(H_c^1(U \otimes_k \bar{k}, \mathcal{F})) \ll \text{cond}(\mathcal{F})^2$$

⁷Recall that the coinvariant space of a representation of a group G is the largest quotient on which the group G acts trivially.

with an absolute implied constant (see, e.g., [32, Chap. 2] or [17, Th. 2.4]).

Finally for $i = 2$, it follows from Poincaré duality that $H_c^2(U \otimes_k \bar{k}, \mathcal{F})$ is isomorphic to the Tate-twisted space of $\pi_1^g(U)$ -coinvariants of $\mathcal{F}_{\bar{\eta}}$ (see, e.g., [32, Chap. 2.]), and hence the contribution of this term is the main term in the formula. \square

6.4.1. Correlation and quasi-orthogonality of trace functions. An important application of the above formula arises when estimating the *correlation* between the trace functions $t_{\mathcal{F}}$ and $t_{\mathcal{G}}$ associated to two admissible sheaves \mathcal{F}, \mathcal{G} , i.e., when computing the sum associated to the tensor product sheaf $\mathcal{F} \otimes \check{\mathcal{G}}$. We define the correlation sum

$$C(\mathcal{F}, \mathcal{G}; k) := \sum_{x \in k} t_{\mathcal{F}}(x; k) \overline{t_{\mathcal{G}}(x; k)}.$$

From (6.3) we have the trivial bound

$$|C_{\mathcal{F}, \mathcal{G}}(k)| \leq \text{cond}(\mathcal{F}) \text{cond}(\mathcal{G}) q.$$

The Riemann Hypothesis allows us improve upon this bound when \mathcal{F}, \mathcal{G} are “disjoint”:

Corollary 6.6 (Square root cancellation). *Let \mathcal{F}, \mathcal{G} be two admissible sheaves on \mathbb{P}_k^1 for a finite field k . If \mathcal{F} and \mathcal{G} have no irreducible constituent in common, then we have*

$$|C(\mathcal{F}, \mathcal{G}; k)| \ll (\text{cond}(\mathcal{F}) \text{cond}(\mathcal{G}))^4 q^{1/2}$$

where the implied constant is absolute. In particular, if in addition $\text{cond}(\mathcal{F})$ and $\text{cond}(\mathcal{G})$ are bounded by a fixed constant, then

$$|C(\mathcal{F}, \mathcal{G}; k)| \ll q^{1/2}.$$

Proof. We have

$$t_{\mathcal{F} \otimes \check{\mathcal{G}}}(x; k) = t_{\mathcal{F}}(x; k) \overline{t_{\mathcal{G}}(x; k)}$$

for $x \in U_{\mathcal{F}}(k) \cap U_{\mathcal{G}}(k)$ and

$$|t_{\mathcal{F} \otimes \check{\mathcal{G}}}(x; k)|, \quad |t_{\mathcal{F}}(x; k) \overline{t_{\mathcal{G}}(x; k)}| \leq \text{cond}(\mathcal{F}) \text{cond}(\mathcal{G}).$$

Thus the previous proposition applied to the sheaf $\mathcal{F} \otimes \check{\mathcal{G}}$ gives

$$\begin{aligned} C(\mathcal{F}, \mathcal{G}; k) &= S(\mathcal{F} \otimes \check{\mathcal{G}}; k) + O((\text{cond}(\mathcal{F}) + \text{cond}(\mathcal{G})) \text{cond}(\mathcal{F}) \text{cond}(\mathcal{G})) \\ &= q \text{Tr} \left(\text{Fr}_k | (\mathcal{F} \otimes \check{\mathcal{G}})_{\bar{\eta}} \right)_{\pi_1^g(U)} + O((\text{cond}(\mathcal{F}) \text{cond}(\mathcal{G}))^4 q^{1/2}) \end{aligned}$$

using (6.5) and (6.6). We conclude by observing that, by Schur’s Lemma and the geometric semisimplicity of admissible sheaves (proved by Deligne [9, (3.4.1)]), our disjointness assumption on \mathcal{F} and \mathcal{G} implies that the coinvariant space vanishes. \square

6.5. The Artin-Schreier sheaf. We will now start discussing specific important admissible sheaves. Let p be a prime and let $\psi: (\mathbb{F}_p, +) \rightarrow \mathbb{C}^\times$ be a non-trivial additive character. For any finite extension k of \mathbb{F}_p , we then have an additive character

$$\psi_k: \begin{cases} k \rightarrow \mathbb{C}^\times \\ x \mapsto \psi(\text{Tr}_{k/\mathbb{F}_p}(x)), \end{cases}$$

where $\text{Tr}_{k/\mathbb{F}_p}$ is the trace map from k to \mathbb{F}_p .

One shows (see [32, Chap. 4], [7, §1.4], [30, p. 302–303]) that there exists an admissible sheaf \mathcal{L}_ψ , called the *Artin-Schreier sheaf* associated to ψ , with the following properties:

- the sheaf \mathcal{L}_ψ has rank 1, hence is automatically geometrically irreducible, and it is geometrically non-trivial;
- the sheaf \mathcal{L}_ψ is lisse on $\mathbb{A}_{\mathbb{F}_p}^1$, and wildly ramified at ∞ with $\text{swan}_\infty(\mathcal{L}_\psi) = 1$, so that in particular $\text{cond}(\mathcal{L}_\psi) = 3$, independently of p and of the non-trivial additive character ψ ;
- the trace function is given by the formula

$$t_{\mathcal{L}_\psi}(x; k) = \psi_k(x)$$

for every finite extension k/\mathbb{F}_p and every $x \in \mathbb{A}^1(k) = k$, and

$$t_{\mathcal{L}_\psi}(\infty; k) = 0.$$

Let $f \in \mathbb{F}_p(X)$ be a rational function not of the shape $g^p - g + c$ for $g \in \mathbb{F}_p(X)$, $c \in \mathbb{F}_p$ (for instance whose zeros or poles have order prime to p). Then f defines a morphism $f: \mathbb{P}_{\mathbb{F}_p}^1 \rightarrow \mathbb{P}_{\mathbb{F}_p}^1$, and we denote by $\mathcal{L}_{\psi(f)}$ the pull-back sheaf $f^*\mathcal{L}_\psi$, which we call the *Artin-Schreier sheaf associated to f and ψ* . Then $\mathcal{L}_{\psi(f)}$ has the following properties:

- it has rank 1, hence is geometrically irreducible, and it is geometrically non-trivial (because f is not of the form $g^p - g + c$ for some other function g , by assumption);
- it is lisse outside the poles of f , and wildly ramified at each pole with Swan conductor equal to the order of the pole, so that if the denominator of f has degree d (coprime to p) we have $\text{cond}(\mathcal{L}_{\psi(f)}) = 1 + e + d$, where e is the number of distinct poles of f ;
- it has trace function given by the formula

$$t_{\mathcal{L}_{\psi(f)}}(x; k) = \psi(\text{tr}_{k/\mathbb{F}_p}(f(x)))$$

for any finite extension k/\mathbb{F}_p and any $x \in \mathbb{P}^1(k)$ which is not a pole of f , and $t_{\mathcal{L}_{\psi(f)}}(x; k) = 0$ if x is a pole of f .

In particular, from Theorem 6.5, we thus obtain the estimate

$$\left| \sum_{x \in \mathbb{F}_p} \psi(f(x)) \right| \ll \deg(f)^2 p^{1/2}$$

for such f , which is a slightly weaker form of the Weil bound from Lemma 4.2. Note that this weakening, which is immaterial in our applications, is only due to the general formulation of Theorem 6.5 which did not attempt to obtain the best possible estimate for specific situations.

6.6. The ℓ -adic Fourier transform. Let p be a prime, k/\mathbb{F}_p a finite extension and ψ a non-trivial additive character of k . For a finite extension k/\mathbb{F}_p and a function $x \mapsto t(x)$ defined on k , we define the *normalized Fourier transform* $\text{FT}_\psi t(x)$ by the formula

$$\text{FT}_\psi t(x) := -\frac{1}{q^{1/2}} \sum_{y \in k} t(y) \psi(xy)$$

(which is similar to (4.11) except for the sign). It is a very deep fact that, when applied to trace functions, this construction has a sheaf-theoretic incarnation. This was defined by Deligne and studied extensively by Laumon [36] and Katz [32]. However, a

restriction on the admissible sheaves is necessary, in view of the following obstruction: if $t(x) = \psi(bx)$ for some $b \in k$, then its Fourier transform is a Dirac-type function

$$\mathrm{FT}_\psi(t)(x) = -q^{1/2}\delta_{-b}(x) = \begin{cases} -q^{1/2} & \text{if } x = -b \\ 0 & \text{otherwise.} \end{cases}$$

But this cannot in general be an admissible trace function with bounded conductor as this would violate (6.2) at $x = -b$ if q is large enough. We make the following definition, as in [32]:

Definition 6.7 (Admissible Fourier sheaves). An admissible sheaf over \mathbb{P}_k^1 is a *Fourier sheaf* if its geometrically irreducible components are neither trivial nor Artin-Schreier sheaves \mathcal{L}_ψ for some non-trivial additive character ψ .

Theorem 6.8 (Sheaf-theoretic Fourier transform). *Let p be a prime and k/\mathbb{F}_p a finite extension, and let ψ be a non-trivial additive character of k . Let \mathcal{F} be an admissible ℓ -adic Fourier sheaf on \mathbb{P}_k^1 . There exists an ℓ -adic sheaf*

$$\mathcal{G} = \mathrm{FT}_\psi(\mathcal{F}),$$

called the Fourier transform of \mathcal{F} , which is also an admissible ℓ -adic Fourier sheaf, with the property that for any finite extension k'/k , we have

$$t_{\mathcal{G}}(\cdot; k') = \mathrm{FT}_{\psi_{k'}} t_{\mathcal{F}}(\cdot; k),$$

in particular

$$t_{\mathcal{G}}(x; k) = -\frac{1}{\sqrt{|k|}} \sum_{y \in k} t_{\mathcal{F}}(y; k) \psi(xy).$$

Moreover, the following additional assertions hold:

- *The sheaf \mathcal{G} is geometrically irreducible, or geometrically isotypic, if and only if \mathcal{F} is;*
- *The Fourier transform is (almost) involutive, in the sense that we have a canonical arithmetic isomorphism*

$$\mathrm{FT}_\psi \mathcal{G} \simeq [\times(-1)]^* \mathcal{F} \tag{6.8}$$

where $[\times(-1)]^$ denotes the pull-back by the map $x \mapsto -x$;*

- *We have*

$$\mathrm{cond}(\mathcal{G}) \leq 10 \mathrm{cond}(\mathcal{F})^2. \tag{6.9}$$

Proof. These claims are established for instance in [32, Chap. 8], with the exception of (6.9) which is proved in [15, Prop. 8.2(1)]. \square

6.7. Kloosterman sheaves. Given a prime $p \geq 3$, a non-trivial additive character ψ of \mathbb{F}_p and an integer $m \geq 1$, the m^{th} hyper-Kloosterman sums are defined by the formula

$$\mathrm{Kl}_m(x; k) := \frac{1}{q^{\frac{m-1}{2}}} \sum_{\substack{y_1, \dots, y_m \in k \\ y_1 \cdots y_m = x}} \psi_k(y_1 + \cdots + y_m) \tag{6.10}$$

for any finite extension k/\mathbb{F}_p and any $x \in k$. Thus, we have for instance $\mathrm{Kl}_1(x; k) = \psi_k(x)$, while Kl_2 is essentially a classical Kloosterman sum.

The following deep result shows that, as functions of x , these sums are trace functions of admissible sheaves.

Proposition 6.9 (Deligne; Katz). *There exists an admissible Fourier sheaf $\mathcal{K}\ell_m$ such that, for any k/\mathbb{F}_p and any $x \in k^\times$, we have*

$$t_{\mathcal{K}\ell_m}(x; k) = (-1)^{m-1} \text{Kl}_m(x; k).$$

Furthermore:

- $\mathcal{K}\ell_m$ is lisse on $\mathbb{G}_m = \mathbb{P}^1 - \{0, \infty\}$; if $m \geq 2$, it is tamely ramified at 0, and for $m = 1$ it is lisse at 0; for all $m \geq 1$, it is wildly ramified at ∞ with Swan conductor 1;
- $\mathcal{K}\ell_m$ is of rank m , and is geometrically irreducible;
- if p is odd, then the Zariski closure of the image $\rho_{\mathcal{K}\ell_m}(\pi_1^g(\mathbb{G}_m))$, which is called the geometric monodromy group of $\mathcal{K}\ell_m$, is isomorphic to SL_m if m is odd, and to Sp_m if m is even.

It follows that $\text{cond}(\mathcal{K}\ell_m) = m + 3$ for all $m \geq 2$ and all p , and that $\text{cond}(\mathcal{K}\ell_1) = 3$.

Proof. All these results can be found in the book of Katz [32]; more precisely, the first two points are part of Theorem 4.1.1 in [32] and the last is part of Theorem 11.1 in the same reference. \square

Remark 6.10. In particular, for $x \neq 0$, we get the estimate

$$|\text{Kl}_m(x; k)| \leq m,$$

first proved by Deligne. Note that this exhibits square-root cancellation in the $(m-1)$ -variable character sum defining $\text{Kl}(x; k)$. For $x = 0$, it is elementary that

$$\text{Kl}_m(0; k) = (-1)^{m-1} q^{-(m-1)/2}.$$

We have the following bounds for hyper-Kloosterman sums, where the case $m = 3$ is the important one for this paper:

Proposition 6.11 (Estimates for hyper-Kloosterman sums). *Let $m \geq 2$ be an integer, and ψ' an additive character of \mathbb{F}_p , which may be trivial. We have*

$$\left| \sum_{x \in \mathbb{F}_p^\times} \text{Kl}_m(x; p) \psi'(x) \right| \ll p^{1/2}. \quad (6.11)$$

Further, let $a \in \mathbb{F}_p^\times$. If either $a \neq 1$ or ψ' is non-trivial, we have

$$\left| \sum_{x \in \mathbb{F}_p^\times} \text{Kl}_m(x; p) \overline{\text{Kl}_m(ax; p)} \psi'(x) \right| \ll p^{1/2} \quad (6.12)$$

In these bounds, the implied constants depend only, and at most polynomially, on m .

Proof. The first bound (6.11) follows directly from Corollary 6.6 and (6.6) because $\mathcal{K}\ell_m$ is, for $m \geq 2$, geometrically irreducible of rank > 1 , and therefore not geometrically isomorphic to the rank 1 Artin-Schreier sheaf $\mathcal{L}_{\psi'}$.

For the proof of (6.12), we use the identity⁸

$$\text{Kl}_m(x) = \frac{1}{p^{1/2}} \sum_{y \in \mathbb{F}_p^\times} \text{Kl}_{m-1}(y^{-1}) \psi(xy) = -\text{FT}_\psi([y^{-1}]^* \text{Kl}_{m-1})(x)$$

⁸One could use this identity to recursively build the hyper-Kloosterman sheaf from the Artin-Schreier sheaf, Theorem 6.8, and pullback via the map $x \mapsto \frac{1}{x}$, if desired.

which is valid for all $x \in \mathbb{F}_p$ (including $x = 0$). If we let $b \in \mathbb{F}_p$ be such that $\psi'(x) = \psi(bx)$ for all x , then by the Plancherel formula, we deduce

$$\begin{aligned} \sum_{x \in \mathbb{F}_p} \text{Kl}_m(x; p) \overline{\text{Kl}_m(ax; p)} \psi'(x) &= \sum_{y \in \mathbb{F}_p \setminus \{0, -b\}} \text{Kl}_{m-1}(y^{-1}) \overline{\text{Kl}_{m-1}(a(y+b)^{-1})} \\ &= \sum_{\substack{y \in \mathbb{F}_p, \\ y \neq 0, -1/b}} \text{Kl}_{m-1}(y; p) \overline{\text{Kl}_{m-1}(\gamma \cdot y; p)} \end{aligned}$$

where

$$\gamma := \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix}.$$

We are in the situation of Corollary 6.6, with both sheaves $\mathcal{K}\ell_{m-1}$ and $\gamma^* \mathcal{K}\ell_{m-1}$ admissible and geometrically irreducible. If $m \geq 3$, $\mathcal{K}\ell_{m-1}$ is tamely ramified at 0 and wildly ramified at ∞ , and $\gamma^* \mathcal{K}\ell_{m-1}$ is therefore tame at $\gamma^{-1}(0)$ and wild at $\gamma^{-1}(\infty)$, so that a geometric isomorphism $\mathcal{K}\ell_{m-1} \simeq \gamma^* \mathcal{K}\ell_{m-1}$ can only occur if $\gamma(0) = 0$ and $\gamma(\infty) = \infty$, or in other words if $b = 0$. If $b = 0$, we have $\gamma^* \mathcal{K}\ell_{m-1} = [\times a]^* \mathcal{K}\ell_{m-1}$ which is known to be geometrically isomorphic to $\mathcal{K}\ell_{m-1}$ if and only if $a = 1$, by [32, Prop. 4.1.5]. Thus (6.12) follows from Corollary 6.6 for $m \geq 3$, using (6.6) and the formulas $\text{cond}(\mathcal{K}\ell_{m-1}) = \text{cond}(\gamma^* \mathcal{K}\ell_{m-1}) = m + 3$.

The case $m = 2$ is easy since the sum above is then simply

$$\sum_{\substack{y \in \mathbb{F}_p, \\ y \neq 0, -1/b}} \psi(y - ay/(by + 1))$$

where the rational function $f(y) = y - ay/(by + 1)$ is constant if and only if $a = 1, b = 0$, so that we can use Lemma 4.2 in this case. \square

Remark 6.12. A similar result was proved by Michel using a different method in [39, Cor. 2.9]. That method requires more information (the knowledge of the geometric monodromy group of $\mathcal{K}\ell_m$) but gives more general estimates. The case $m = 3$ is (somewhat implicitly) the result used by Friedlander and Iwaniec in [21], which is proved by Birch and Bombieri in the Appendix to [21] (with in fact two proofs, which are rather different and somewhat more ad-hoc than the argument presented here). This same estimate is used by Zhang [52] to control Type III sums.

6.8. The van der Corput method for trace functions. Let $t = t_{\mathcal{F}}$ be the trace function associated to an admissible sheaf \mathcal{F} . In the spirit of Proposition 4.12, the q -van der Corput method, when applied to incomplete sums of t , followed by completion of sums, produces expressions of the form

$$\sum_{x \in \mathbb{F}_p} t(x) \overline{t(x+l)} \psi(hx)$$

for $(h, l) \in \mathbb{F}_p \times \mathbb{F}_p^\times$, and for some additive character ψ . We seek sufficient conditions that ensure square-root cancellation in the above sum, for any $l \neq 0$ and any h .

Observe that if

$$t(x) = \psi(ax^2 + bx),$$

then the sum is sometimes of size p . Precisely, this happens if and only if $h = 2al$. As we shall see, this phenomenon is essentially the only obstruction to square-root cancellation.

Definition 6.13 (No polynomial phase). For a finite field k and $d \geq 0$, we say that an admissible sheaf \mathcal{F} over \mathbb{P}_k^1 has *no polynomial phase* of degree $\leq d$ if no geometrically irreducible component of \mathcal{F} is geometrically isomorphic to a sheaf of the form $\mathcal{L}_{\psi(P(x))}$ where $P(X) \in \mathbb{F}_p[X]$ is a polynomial of degree $\leq d$.

Thus, for instance, an admissible sheaf is Fourier if and only if it has no polynomial phase of degree ≤ 1 .

Remark 6.14. An obvious sufficient condition for \mathcal{F} not to contain any polynomial phase (of any degree) is that each geometrically irreducible component of \mathcal{F} be irreducible of rank ≥ 2 , for instance that \mathcal{F} itself be geometrically irreducible of rank ≥ 2 .

The following inverse theorem is a variant of an argument of Fouvry, Kowalski and Michel [17, Lemma 5.4].

Theorem 6.15. *Let $d \geq 1$ be an integer, and let p be a prime such that $p > d$. Let \mathcal{F} be an isotypic admissible sheaf over $\mathbb{P}_{\mathbb{F}_p}^1$ with no polynomial phase of degree $\leq d$. Then either $\text{cond}(\mathcal{F}) \geq p + 1$, or for any $l \in \mathbb{F}_p^\times$ the sheaf $\mathcal{F} \otimes [+l]^* \check{\mathcal{F}}$ contains no polynomial phase of degree $\leq d - 1$.*

In all cases, for any $l \in \mathbb{F}_p^\times$ and any $P(X) \in \mathbb{F}_p[X]$ of degree $d - 1$, we have

$$\left| \sum_{x \in \mathbb{F}_p} t_{\mathcal{F}}(x + l) \overline{t_{\mathcal{F}}(x)} \psi(P(x)) \right| \ll p^{1/2} \quad (6.13)$$

where the implied constant depends, at most polynomially, on $\text{cond}(\mathcal{F})$ and on d . Furthermore, this estimate holds also if $l = 0$ and $P(x) = hx$ with $h \neq 0$.

Proof. First suppose that $l \neq 0$. Observe that if $\text{cond}(\mathcal{F}) \geq p + 1$, the bound (6.13) follows from the trivial bound

$$|t_{\mathcal{F}}(x + l) \overline{t_{\mathcal{F}}(x)} \psi(P(x))| \leq \text{rk}(\mathcal{F})^2 \leq \text{cond}(\mathcal{F})^2,$$

and that if the sheaf $[+l]^* \mathcal{F} \otimes \check{\mathcal{F}}$ contains no polynomial phase of degree $\leq d - 1$, then the bound is a consequence of Corollary 6.6.

We now prove that one of these two properties holds. We assume that $[+l]^* \mathcal{F} \otimes \check{\mathcal{F}}$ contains a polynomial phase of degree $\leq d - 1$, and will deduce that $\text{cond}(\mathcal{F}) \geq p + 1$.

Since \mathcal{F} is isotypic, the assumption implies that there is a geometric isomorphism

$$[+l]^* \mathcal{F} \simeq \mathcal{F} \otimes \mathcal{L}_{\psi(P(x))}$$

for some polynomial $P(X) \in \mathbb{F}_p[X]$ of degree $\leq d - 1$. Then, considering the geometric irreducible component \mathcal{G} of \mathcal{F} (which is a sheaf on $\mathbb{P}_{\mathbb{F}_p}^1$) we also have

$$[+l]^* \mathcal{G} \simeq \mathcal{G} \otimes \mathcal{L}_{\psi(P(x))}. \quad (6.14)$$

If \mathcal{G} is ramified at some point $x \in \mathbb{A}^1(\bar{k})$, then since $\mathcal{L}_{\psi(P(x))}$ is lisse on $\mathbb{A}^1(\bar{k})$, we conclude by iterating (6.14) that \mathcal{G} is ramified at $x, x + l, x + 2l, \dots, x + (p - 1)l$, which implies that $\text{cond}(\mathcal{F}) \geq \text{cond}(\mathcal{G}) \geq p + \text{rk}(\mathcal{G})$. Thus there remains to handle the case when \mathcal{G} is lisse outside ∞ . It then follows from [17, Lemma 5.4 (2)] that either $\text{cond}(\mathcal{G}) \geq \text{rk}(\mathcal{G}) + p$, in which case $\text{cond}(\mathcal{F}) \geq p + 1$ again, or that \mathcal{G} is isomorphic (over \mathbb{F}_p) to a sheaf of the form $\mathcal{L}_{\psi(Q(x))}$ for some polynomial of degree $\leq d$. Since \mathcal{G} is a geometrically irreducible component of \mathcal{F} , this contradicts the assumption on \mathcal{F} .

Finally, consider the case where $l = 0$ and $P(x) = hx$ with $h \neq 0$. Using Corollary 6.6 and (6.6), the result holds for a given $h \in \mathbb{F}_p^\times$ unless the geometrically irreducible component \mathcal{G} of \mathcal{F} satisfies

$$\mathcal{G} \simeq \mathcal{G} \otimes \mathcal{L}_{\psi(hx)}.$$

Since $d \geq 1$, \mathcal{F} is a Fourier sheaf, and hence so are \mathcal{G} and $\mathcal{G} \otimes \mathcal{L}_{\psi(hx)}$. Taking the Fourier transform of both sides of this isomorphism, we obtain easily

$$[+h]^* \text{FT}_\psi \mathcal{G} \simeq \text{FT}_\psi \mathcal{G}$$

and it follows from [17, Lemma 5.4 (2)] again that $\text{cond}(\text{FT}_\psi \mathcal{G}) \geq p + 1$. Using the Fourier inversion formula (6.8) and (6.9), we derive

$$\text{cond}(\mathcal{F}) \geq \text{cond}(\mathcal{G}) \gg p^{1/2},$$

so that the bound (6.13) also holds trivially in this case. \square

Remark 6.16. For later use, we observe that the property of having *no polynomial phase of degree ≤ 2* of an admissible sheaf \mathcal{F} is invariant under the following transformations:

- Twists by an Artin-Schreier sheaf associated to a polynomial phase of degree ≤ 2 , i.e., $\mathcal{F} \mapsto \mathcal{F} \otimes \mathcal{L}_{\psi(ax^2+bx)}$;
- Dilations and translations: $\mathcal{F} \mapsto [\times a]^* \mathcal{F}$ and $\mathcal{F} \mapsto [+b]^* \mathcal{F}$ where $a \in \mathbb{F}_p^\times$ and $b \in \mathbb{F}_p$;
- Fourier transforms, if \mathcal{F} is Fourier: $\mathcal{F} \mapsto \text{FT}_\psi \mathcal{F}$. Indeed, the Fourier transform of a sheaf $\mathcal{L}_{\psi(P(x))}$ with $\deg(P) = 2$ is geometrically isomorphic to $\mathcal{L}_{\psi(Q(x))}$ for some polynomial Q of degree 2.

6.9. Study of some specific exponential sums. We now apply the theory above to some specific multi-dimensional exponential sums which appear in the refined treatment of the Type I sums in Section 8. For parameters $(a, b, c, d, e) \in \mathbb{F}_p$, with $a \neq c$, we consider the rational function

$$f(X, Y) := \frac{1}{(Y + aX + b)(Y + cX + d)} + eY \in \mathbb{F}_p(X, Y).$$

For a fixed non-trivial additive character ψ of \mathbb{F}_p and for any $x \in \mathbb{F}_p$, we define the character sum

$$K_f(x; p) := -\frac{1}{p^{1/2}} \sum_{\substack{y \in \mathbb{F}_p \\ (y+ax+b)(y+cx+d) \neq 0}} \psi(f(x, y)). \quad (6.15)$$

For any $x \in \mathbb{F}_p$, the specialized rational function $f(x, Y) \in \mathbb{F}_p(Y)$ is non-constant (it has poles in $\mathbb{A}_{\mathbb{F}_p}^1$), and therefore by Lemma 4.2 (or Theorem 6.5) we have

$$|K_f(x; p)| \leq 4 \quad (6.16)$$

We will prove the following additional properties of the sums $K_f(x; p)$:

Theorem 6.17. *For a prime p and parameters $(a, b, c, d, e) \in \mathbb{F}_p^5$ with $a \neq c$, the function $x \mapsto K_f(x; p)$ on \mathbb{F}_p is the trace function of an admissible geometrically irreducible sheaf \mathcal{F} whose conductor is bounded by a constant independent of p . Furthermore, \mathcal{F} contains no polynomial phase of degree ≤ 2 .*

In particular, we have

$$\left| \sum_{x \in \mathbb{F}_p} K_f(x; p) \psi(hx) \right| \ll p^{1/2} \quad (6.17)$$

for all $h \in \mathbb{F}_p$ and

$$\left| \sum_{x \in \mathbb{F}_p} K_f(x; p) \overline{K_f(x + l; p)} \psi(hx) \right| \ll p^{1/2} \quad (6.18)$$

for any $(h, l) \in \mathbb{F}_p^2 - \{(0, 0)\}$, where the implied constants are absolute.

Proof. Note that the estimates (6.17) and (6.18) follow from the first assertion (see Theorem 6.15).

We first normalize most of the parameters: we have

$$K_f(x; p) = -\frac{\psi(-eax - eb)}{p^{1/2}} \sum_{z \in \mathbb{F}_p} \psi\left(ez + \frac{1}{z(z + (c - a)x + d - b)}\right),$$

and by Remark 6.16, this means that we may assume that $c = d = 0$, $a \neq 0$. Furthermore, we have then

$$K_f(x; p) = K_{\tilde{f}}(ax + b; p)$$

where \tilde{f} is the rational function f with parameters $(1, 0, 0, 0, e)$. Again by Remark 6.16, we are reduced to the special case $f = \tilde{f}$, i.e., to the sum

$$K_f(x; p) = -\frac{1}{p^{1/2}} \sum_{\substack{y \in \mathbb{F}_p \\ (y+x)y \neq 0}} \psi\left(\frac{1}{(y+x)y} + ey\right).$$

We will prove that the Fourier transform of K_f is the trace function of a geometrically irreducible Fourier sheaf with bounded conductor and no polynomial phase of degree ≤ 2 . By the Fourier inversion formula (6.8) and (6.9), and the invariance of the property of not containing a polynomial phase of degree ≤ 2 under Fourier transform (Remark 6.16 again), this will imply the result for K_f .

For $z \in \mathbb{F}_p$, we have

$$\text{FT}_\psi(K_f)(z) = \frac{1}{p} \sum_{y+x, y \neq 0} \sum \psi\left(\frac{1}{(y+x)y} + ey + zx\right)$$

If $z \neq 0$, the change of variables

$$y_1 := \frac{1}{(y+x)y}, \quad y_2 := z(y+x)$$

is a bijection

$$\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y(x+y) \neq 0\} \rightarrow \{(y_1, y_2) \in \mathbb{F}_p^\times \times \mathbb{F}_p^\times\}$$

(with inverse $y = z/(y_1 y_2)$ and $x = y_2/z - z/(y_1 y_2)$), which satisfies

$$\frac{1}{(y+x)y} + ey + zx = y_1 + \frac{ez}{y_1 y_2} + y_2 - \frac{z^2}{y_1 y_2} = y_1 + y_2 + \frac{z(e-z)}{y_1 y_2}$$

for $y(x+y) \neq 0$. Thus

$$\text{FT}_\psi(K_f)(z) = \frac{1}{p} \sum_{y_1, y_2 \in \mathbb{F}_p^\times} \sum \psi\left(y_1 + y_2 + \frac{z(e-z)}{y_1 y_2}\right) = \text{Kl}_3(z(e-z); p)$$

for $z(e-z) \neq 0$.

Similar calculations reveal that this identity also holds when $z = 0$ and $z = e$ (treating the doubly degenerate case $z = e = 0$ separately), i.e., both sides are equal to $\frac{1}{p}$ in these cases. This means that $\mathrm{FT}_\psi(K_f)$ is the trace function of the pullback sheaf

$$\mathcal{G}_f := \varphi^* \mathcal{K}\ell_3,$$

where φ is the quadratic map $\varphi : z \mapsto z(e - z)$.

The sheaf \mathcal{G}_f has bounded conductor (it has rank 3 and is lisse on $U = \mathbb{P}_{\mathbb{F}_p}^1 - \{0, e, \infty\}$, with wild ramification at ∞ only, where the Swan conductor can be estimated using [32, 1.13.1], for $p \geq 3$). We also claim that \mathcal{G}_f is geometrically irreducible. Indeed, it suffices to check that $\pi_1^g(U)$ acts irreducibly on the underlying vector space of $\rho_{\mathcal{K}\ell_3}$. But since $z \mapsto z(e - z)$ is a non-constant morphism $\mathbb{P}_{\mathbb{F}_p}^1 \rightarrow \mathbb{P}_{\mathbb{F}_p}^1$, $\pi_1^g(U)$ acts by a finite-index subgroup of the action of $\pi_1^g(\mathbb{G}_m)$ on $\mathcal{K}\ell_3$. Since the image of $\pi_1^g(\mathbb{G}_m)$ is Zariski-dense in SL_3 (as recalled in Proposition 6.9), which is a connected algebraic group, it follows that the image of $\pi_1^g(U)$ is also Zariski-dense in SL_3 , proving the irreducibility.

Since \mathcal{G}_f is geometrically irreducible of rank $3 > 1$, it does not contain any polynomial phase (see Remark 6.14), concluding the proof. \square

Remark 6.18. Another natural strategy for proving this theorem would be to start with the observation that the function $x \mapsto K_f(x; k)$ is the trace function of the constructible ℓ -adic sheaf

$$\mathcal{K}_f = R^1 \pi_{1,!} \mathcal{L}_{\psi(f)}(1/2), \quad \mathcal{L}_{\psi(f)} = f^* \mathcal{L}_\psi$$

where $\pi_1 : \mathbb{A}_{\mathbb{F}_p}^2 \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$ is the projection on the first coordinate and $R^1 \pi_{1,!}$ denotes the operation of higher-direct image with compact support associated to that map (and $(1/2)$ is a Tate twist). This is known to be mixed of weights ≤ 0 by Deligne's work [9], and it follows from the general results⁹ of Fouvry, Kowalski and Michel in [19] that the conductor of this sheaf is absolutely bounded as p varies. To fully implement this approach, it would still remain to prove that the weight 0 part of \mathcal{K}_f is geometrically irreducible with no polynomial phase of degree ≤ 2 . Although such arguments might be necessary in more advanced cases, the direct approach we have taken is simpler here.

Remark 6.19. In the remainder of this paper, we will only use the bounds (6.17) and (6.18) from Theorem 6.17. These bounds can also be expressed in terms of the Fourier transform $\mathrm{FT}_\psi(K_f)$ of K_f , since they are equivalent to

$$|\mathrm{FT}_\psi(K_f)(h)| \ll p^{1/2}$$

and

$$\left| \sum_{x \in \mathbb{F}_p} \mathrm{FT}_\psi(K_f)(x + h) \overline{\mathrm{FT}_\psi(K_f)(x)} \psi(-lx) \right| \ll p^{1/2},$$

respectively. As such, we see that it is in fact enough to show that $\mathrm{FT}_\psi(K_f)$, rather than K_f , is the trace function of a geometrically irreducible admissible sheaf with bounded conductor and no quadratic phase component. Thus, in principle, we could avoid any use of Theorem 6.8 in our arguments (provided that we took the existence of the Kloosterman sheaves for granted). However, from a conceptual point of view, the fact that K_f has a good trace function interpretation is more important than the corresponding fact for FT_ψ (for instance, the iterated van der Corput bounds in Remark 6.23 rely on the former fact rather than the latter).

⁹Which were partly motivated by the current paper.

6.10. Incomplete sums of trace functions. In this section, we extend the discussion of Section 4 to general admissible trace functions. More precisely, given a squarefree integer q , we say that a q -periodic arithmetic function

$$t: \mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{C}$$

is an *admissible trace function* if we have

$$t(x) = \prod_{p|q} t(x; p) \quad (6.19)$$

for all x where, for each prime $p \mid q$, $x \mapsto t(x; p)$ is the composition of reduction modulo p and the trace function associated to an admissible sheaf \mathcal{F}_p on $\mathbb{P}_{\mathbb{F}_p}^1$.

An example is the case discussed in Section 4: for a rational function $f(X) = P(X)/Q(X) \in \mathbb{Q}(X)$ with $P, Q \in \mathbb{Z}[X]$ and a squarefree integer q such that $Q(q) \neq 0$, we can write

$$e_q(f(x)) = e_q\left(\frac{P(x)}{Q(x)}\right) = \prod_{p|q} e_p(\overline{q_p}f(x)), \quad \text{where } q_p = q/p.$$

(by Lemma 4.4). In that case, we take

$$\mathcal{F}_p = \mathcal{L}_{\psi(f)}, \quad \text{where } \psi(x) = e_p(\overline{q_p}x).$$

Another example is given by the Kloosterman sums defined for q squarefree and $x \in \mathbb{Z}$ by

$$\text{Kl}_m(x; q) = \frac{1}{q^{m-1/2}} \sum_{\substack{x_1, \dots, x_m \in \mathbb{Z}/q\mathbb{Z} \\ x_1 \cdots x_m = x}} e_q(x_1 + \cdots + x_m), \quad (6.20)$$

for which we have

$$\text{Kl}_m(x; q) = \prod_{p|q} \text{Kl}_m(\overline{q_p}^m x; p) = \prod_{p|q} ([\times \overline{q_p}^m]^* \text{Kl}_m(\cdot; p))(x).$$

and hence

$$\text{Kl}_m(x; q) = (-1)^{(m-1)\Omega(q)} t(x)$$

where

$$t(x) = \prod_{p|q} (-1)^{m-1} t_{\mathcal{F}_p}(x; p) \text{ with } \mathcal{F}_p = [\times \overline{q_p}^m]^* \mathcal{K} \ell_m$$

is an admissible trace function modulo q .

Given a tuple of admissible sheaves $\mathcal{F} = (\mathcal{F}_p)_{p|q}$, we define the conductor $\text{cond}(\mathcal{F})$ as

$$\text{cond}(\mathcal{F}) = \prod_{p|q} \text{cond}(\mathcal{F}_p).$$

Thus, for the examples above, the conductor is bounded by $C^{\Omega(q)}$ for some constant C depending only on f (resp. on m). This will be a general feature in applications.

6.10.1. *A generalization of Proposition 4.12.* Thanks to the square root cancellation for complete sums of trace functions provided by Corollary 6.6, we may extend Proposition 4.12 to general admissible trace functions to squarefree moduli.

Proposition 6.20 (Incomplete sum of trace function). *Let q be a squarefree natural number of polynomial size and let $t(\cdot; q): \mathbb{Z} \rightarrow \mathbb{C}$ be an admissible trace function modulo q associated to admissible sheaves $\mathcal{F} = (\mathcal{F}_p)_{p|q}$.*

Let further $N \geq 1$ be given with $N \ll q^{O(1)}$ and let ψ_N be a function on \mathbb{R} defined by

$$\psi_N(x) = \psi\left(\frac{x - x_0}{N}\right)$$

where $x_0 \in \mathbb{R}$ and ψ is a smooth function with compact support satisfying

$$|\psi^{(j)}(x)| \ll \log^{O(1)} N$$

for all fixed $j \geq 0$, where the implied constant may depend on j .

(i) (Pólya-Vinogradov + Deligne) *Assume that, for every $p|q$, the sheaf \mathcal{F}_p has no polynomial phase of degree ≤ 1 . Then we have*

$$\left| \sum_n \psi_N(n) t(n; q) \right| \ll q^{1/2+\varepsilon} \left(1 + \frac{N}{q}\right). \quad (6.21)$$

for any $\varepsilon > 0$.

(ii) (one van der Corput + Deligne) *Assume that, for every $p|q$, the sheaf \mathcal{F}_p has no polynomial phase of degree ≤ 2 . Then, for any factorization $q = rs$ and $N \leq q$, we have*

$$\left| \sum_n \psi_N(n) t(n; q) \right| \ll q^\varepsilon \left(N^{1/2} r^{1/2} + N^{1/2} s^{1/4} \right). \quad (6.22)$$

In all cases the implied constants depend on ε , $\text{cond}(\mathcal{F})$ and the implied constants in the estimates for the derivatives of ψ .

Remark 6.21. In the context of Proposition 4.12, where $t(n; q) = e_q\left(\frac{P(n)}{Q(n)}\right)$, the assumptions $\deg P < \deg Q$ and $\deg(Q(p)) = \deg(Q)$ (for all $p \mid q$), ensure that the sheaves $\mathcal{L}_{e_p\left(\frac{P(x)}{Q(x)}\right)}$ do not contain any polynomial phase of any degree.

Remark 6.22. For future reference, we observe that, in the proof of (6.22) below, we will not use any of the properties of the functions $x \mapsto t(x; p)$ for $p \mid r$ for a given factorization $q = rs$, except for their boundedness.

Proof. For each $p \mid q$, the trace function $t_{\mathcal{F}_p}$ decomposes by (6.7) into a sum of at most $\text{rk}(\mathcal{F}_p) \leq \text{cond}(\mathcal{F}_p) \leq \text{cond}(\mathcal{F})$ trace functions of isotypic admissible sheaves, and therefore $n \mapsto t(n; q)$ decomposes into a sum of at most $C^{\omega(q)}$ functions, each of which is an admissible trace function modulo q associated to isotypic admissible sheaves. Moreover, if no \mathcal{F}_p contains a polynomial phase of degree $\leq d$, then all isotypic components share this property (in particular, since $d \geq 1$ for both statements, each component is also a Fourier sheaf). Thus we may assume without loss of generality that each \mathcal{F}_p is isotypic.

We start with the proof of (6.21). By (4.12) we have

$$\begin{aligned} \left| \sum_n \psi_N(n) t(n; q) \right| &\ll q^{1/2+\varepsilon} \left(1 + \frac{|N'|}{q} \right) \sup_{h \in \mathbb{Z}/q\mathbb{Z}} |\mathrm{FT}_q(t(h; q))| \\ &\ll q^{1/2+\varepsilon} \left(1 + \frac{N}{q} \right) \sup_{h \in \mathbb{Z}/q\mathbb{Z}} |\mathrm{FT}_q(t(h; q))| \end{aligned}$$

for any $\varepsilon > 0$, where $N' = \sum_n \psi_N(n)$. By Lemma 4.4, (6.19) and the definition of the Fourier transform, we have

$$\mathrm{FT}_q(t(\cdot; q))(h) = \prod_{p|q} \mathrm{FT}_p(t(\cdot; p))(\overline{q_p}h).$$

Since $t(\cdot; p) = t_{\mathcal{F}_p}$ is the trace function of a Fourier sheaf, we have

$$|\mathrm{FT}_p(t(\cdot; p))(\overline{q_p}h)| \leq 10 \mathrm{cond}(\mathcal{F}_p)^2 \leq 10 \mathrm{cond}(\mathcal{F})^2$$

for all h by (6.9) (or Corollary 6.6 applied to the sheaves \mathcal{F}_p and $\mathcal{L}_{e_p(-\overline{q_p}x)}$). Combining these bounds, we obtain (6.21).

The proof of (6.22) follows closely that of (4.20). It is sufficient to prove this bound in the case $r \leq s$. We may also assume that $r \leq N \leq s$, since, otherwise, the result follows either from the trivial bound or (6.21). Then, denoting $K := \lfloor N/r \rfloor$, we write

$$\sum_n \psi_N(n) t(n; q) = \frac{1}{K} \sum_n \sum_{k=1}^K \psi_N(n + kr) t(n + kr; q).$$

Since $q = rs$, we have

$$t(n + kr; q) = t(n; r) t(n + kr; s),$$

where

$$t(n; r) = \prod_{p|r} t(n; p), \quad t(n; s) = \prod_{p|s} t(n; p)$$

are admissible trace functions modulo r and s , respectively. Hence

$$\begin{aligned} \left| \sum_n \psi_N(n) t(n; q) \right| &\ll \frac{1}{K} \sum_n \left| \sum_{k=1}^K \psi_N(n + kr) t(n + kr; s) \right| \\ &\ll \frac{N^{1/2}}{K} \left(\sum_n \left| \sum_{k=1}^K \psi_N(n + kr) t(n + kr; s) \right|^2 \right)^{1/2} \\ &\ll \frac{N^{1/2}}{K} \left(\sum_{1 \leq k, l \leq K} A(k, l) \right)^{1/2}, \end{aligned}$$

where

$$A(k, l) = \sum_n \psi_N(n + kr) \overline{\psi_N(n + lr)} t(n + kr; s) \overline{t(n + lr; s)}.$$

The diagonal contribution satisfies

$$\sum_{1 \leq k \leq K} A(k, k) \ll q^\varepsilon K N$$

for any $\varepsilon > 0$, where the implied constant depends on $\mathrm{cond}(\mathcal{F})$.

Instead of applying (6.21) for the off-diagonal terms, it is slightly easier to just apply (4.12). For given $k \neq l$, since $kr, lr \ll N$, the sequence $\Psi_N(n) = \psi_N(n + kr)\overline{\psi_N(n + lr)}$ satisfies the assumptions of (4.12). Denoting

$$w(n; s) = t(n + kr; s)\overline{t(n + lr; s)},$$

we obtain

$$|A(k, l)| = \left| \sum_n \Psi_N(n) w(n; s) \right| \ll q^\varepsilon s^{1/2} \sup_{h \in \mathbb{Z}/s\mathbb{Z}} |\text{FT}_s(w(\cdot; s))(h)|$$

by (4.12) (since $N \leq s$). We have

$$\text{FT}_s(w(\cdot; s))(h) = \prod_{p|s} \text{FT}_p(w(\cdot; p))(\overline{s_p}h)$$

with $s_p = s/p$. For $p \mid k - l$, we use the trivial bound

$$|\text{FT}_p(w(\cdot; p))(\overline{s_p}h)| \ll p^{1/2}$$

and for $p \nmid k - l$, we have

$$\text{FT}_p(w(\cdot; p))(\overline{s_p}h) = \frac{1}{p^{1/2}} \sum_{x \in \mathbb{F}_p} t(x + kr; p) \overline{t(x + lr; p)} e_p(\overline{s_p}hx) \ll 1$$

by the change of variable $x \mapsto x + kq_1$ and (6.13), which holds for \mathcal{F}_p by our assumptions. In all cases, the implied constant depends only on $\text{cond}(\mathcal{F}_p)$. Therefore we have

$$A(k, l) \ll (k - l, s)^{1/2} q^\varepsilon s^{1/2},$$

and summing over $k \neq l$, we derive

$$\begin{aligned} \left| \sum_n \psi_N(n) e_q(f(n)) \right| &\ll \frac{q^\varepsilon N^{1/2}}{K} \left(KN + s^{1/2} \sum_{1 \leq k \neq l \leq K} (k - l, s)^{1/2} \right)^{1/2} \\ &\ll \frac{q^\varepsilon N^{1/2}}{K} (K^{1/2} N^{1/2} + s^{1/4} K) \end{aligned}$$

which gives the desired conclusion (6.22). \square

Remark 6.23. Similarly to Remark 4.15, one can iterate the above argument and conclude that, for any $l \geq 1$, and any factorization $q = q_1 \cdots q_l$

$$\left| \sum_n \psi_N(n) t(n; q) \right| \ll q^\varepsilon \left(\left(\sum_{i=1}^{l-1} N^{1-1/2^i} q_i^{1/2^i} \right) + N^{1-1/2^{l-1}} q_l^{1/2^l} \right),$$

assuming that $N < q$ and the \mathcal{F}_p do not contain any polynomial phase of degree $\leq l$.

Specializing Proposition 6.20 to the functions in Theorem 6.17, we conclude:

Corollary 6.24. *Let $q \geq 1$ be a squarefree integer and let $K(\cdot; q)$ be given by*

$$K(x; q) := \frac{1}{q^{1/2}} \sum_{y \in \mathbb{Z}/q\mathbb{Z}} e_q(f(x, y))$$

where

$$f(x, y) = \frac{1}{(y + ax + b)(y + cx + d)} + ey$$

and a, b, c, d, e are integers with $(a - c, q) = 1$. Let further $N \geq 1$ be given with $N \ll q^{O(1)}$ and let ψ_N be a function on \mathbb{R} defined by

$$\psi_N(x) = \psi\left(\frac{x - x_0}{N}\right)$$

where $x_0 \in \mathbb{R}$ and ψ is a smooth function with compact support satisfying

$$|\psi^{(j)}(x)| \ll \log^{O(1)} N$$

for all fixed $j \geq 0$, where the implied constant may depend on j .

Then we have

$$\left| \sum_n \psi_N(n) K(n; q) \right| \ll q^{1/2+\varepsilon} \left(1 + \frac{N}{q} \right) \quad (6.23)$$

for any $\varepsilon > 0$.

Furthermore, for any factorization $q = rs$ and $N \leq q$, we have the additional bound

$$\left| \sum_n \psi_N(n) K(n; q) \right| \ll q^\varepsilon \left(N^{1/2} r^{1/2} + N^{1/2} s^{1/4} \right). \quad (6.24)$$

Indeed, it follows from Theorem 6.17 and the assumption $(a - c, q) = 1$ that $K_f(\cdot; q)$ is an admissible trace function modulo q associated to sheaves which do not contain any polynomial phase of degree ≤ 2 .

6.10.2. Correlations of hyper-Kloosterman sums of composite moduli. Finally, we extend Proposition 6.11 to composite moduli:

Lemma 6.25 (Correlation of hyper-Kloosterman sums). *Let s, r_1, r_2 be squarefree integers with $(s, r_1) = (s, r_2) = 1$. Let $a_1 \in (\mathbb{Z}/r_1 s)^\times$, $a_2 \in (\mathbb{Z}/r_2 s)^\times$, and $n \in \mathbb{Z}/([r_1, r_2]s)\mathbb{Z}$. Then we have*

$$\sum_{h \in (\mathbb{Z}/s[r_1, r_2]\mathbb{Z})^\times} \text{Kl}_3(a_1 h; r_1 s) \overline{\text{Kl}_3(a_2 h; r_2 s)} e_{[r_1, r_2]s}(nh) \ll$$

$$(s[r_1, r_2])^\varepsilon s^{1/2} [r_1, r_2]^{1/2} (a_2 - a_1, n, r_1, r_2)^{1/2} (a_2 r_1^3 - a_1 r_2^3, n, s)^{1/2}$$

for any $\varepsilon > 0$, where the implied constant depends only on ε .

Proof. Let S be the sum to estimate. From Lemma 4.4, we get

$$\text{Kl}_3(a_i h; r_i s) = \text{Kl}_3(a_i \bar{s}^3 h; r_i) \text{Kl}_3(a_i \bar{r}_i^3 h; s)$$

for $i = 1, 2$, as well as

$$e_{[r_1, r_2]s}(nh) = e_{[r_1, r_2]}(\bar{s}nh) e_s(\overline{[r_1, r_2]}nh).$$

and therefore $S = S_1 S_2$ with

$$S_1 = \sum_{h \in (\mathbb{Z}/[r_1, r_2]\mathbb{Z})^\times} \text{Kl}_3(a_1 \bar{s}^3 h; r_1) \overline{\text{Kl}_3(a_2 \bar{s}^3 h; r_2)} e_{[r_1, r_2]}(\bar{s}nh),$$

$$S_2 = \sum_{h \in (\mathbb{Z}/s\mathbb{Z})^\times} \text{Kl}_3(a_1 \bar{r}_1^3 h; s) \overline{\text{Kl}_3(a_2 \bar{r}_2^3 h; s)} e_s(\overline{[r_1, r_2]}nh).$$

Splitting further the summands as products over the primes dividing $[r_1, r_2]$ and s , respectively, we see that it is enough to prove the estimate

$$\left| \sum_{h \in (\mathbb{Z}/p\mathbb{Z})^\times} \text{Kl}_3(b_1 h; d_1) \overline{\text{Kl}_3(b_2 h; d_2)} e_p(mh) \right| \ll p^{1/2} (b_1 - b_2, m, d_1, d_2)^{1/2} \quad (6.25)$$

for p prime and integers $d_1, d_2 \geq 1$ such that $[d_1, d_2] = p$ is prime, and for all $m \in \mathbb{Z}/p\mathbb{Z}$, and $b_1, b_2 \in (\mathbb{Z}/p\mathbb{Z})^\times$.

We now split into cases. First suppose that $d_2 = 1$, so that $d_1 = p$. Then we have $\text{Kl}_3(b_2 h; d_2) = 1$, and the left-hand side of (6.25) simplifies to

$$\sum_{h \in (\mathbb{Z}/p\mathbb{Z})^\times} \text{Kl}_3(b_1 h; p) e_p(mh) \ll p^{1/2}$$

by the first part of Proposition 6.11. Similarly, we obtain (6.25) if $d_1 = 1$.

If $d_1 = d_2 = p$ and $b_1 - b_2 = m = 0 \pmod{p}$, then the claim follows from the bound $|\text{Kl}_3(h; p)| \ll 1$ (see Remark 6.10).

Finally, if $d_1 = d_2 = p$ and $b_1 - b_2 \neq 0 \pmod{p}$ or $m \neq 0 \pmod{p}$, then (6.25) is a consequence of the second part of Proposition 6.11. \square

Finally, from this result, we obtain the following corollary:

Corollary 6.26 (Correlation of hyper-Kloosterman sums, II). *Let s, r_1, r_2 be squarefree integers with $(s, r_1) = (s, r_2) = 1$. Let $a_1 \in (\mathbb{Z}/r_1 s)^\times$, $a_2 \in (\mathbb{Z}/r_2 s)^\times$. Let further $H \geq 1$ be given with $H \ll (s[r_1, r_2])^{O(1)}$ and let ψ_H be a function on \mathbb{R} defined by*

$$\psi_H(x) = \psi\left(\frac{x - x_0}{H}\right)$$

where $x_0 \in \mathbb{R}$ and ψ is a smooth function with compact support satisfying

$$|\psi^{(j)}(x)| \ll \log^{O(1)} H$$

for all fixed $j \geq 0$, where the implied constant may depend on j . Then we have

$$\left| \sum_{(h, s[r_1, r_2])=1} \Psi_H(h) \text{Kl}_3(a_1 h; r_1 s) \overline{\text{Kl}_3(a_2 h; r_2 s)} \right| \ll (s[r_1, r_2])^\varepsilon \left(\frac{H}{[r_1, r_2]s} + 1 \right) s^{1/2} [r_1, r_2]^{1/2} (a_2 - a_1, r_1, r_2)^{1/2} (a_2 r_1^3 - a_1 r_2^3, s)^{1/2}$$

for any $\varepsilon > 0$ and any integer n .

This exponential sum estimate will be the main estimate used for controlling Type III sums in Section 7.

Proof. This follows almost directly from Lemma 6.25 and the completion of sums in Lemma 4.9, except that we must incorporate the restriction $(h, s[r_1, r_2]) = 1$. We do this using Möbius inversion: the sum S to estimate is equal to

$$\sum_{\delta | s[r_1, r_2]} \mu(\delta) t_1(\delta) S_1(\delta)$$

where $t_1(\delta)$ satisfies $|t_1(\delta)| \leq \delta^{-2}$ because $\text{Kl}_3(0; p) = p^{-1}$ for any prime p , and

$$\begin{aligned} S_1(\delta) &= \sum_{\delta | h} \Psi_H(h) \text{Kl}_3(\alpha_1 h; r_1 s / (\delta, r_1 s)) \overline{\text{Kl}_3(\alpha_2 h; r_2 s / (\delta, r_2 s))} \\ &= \sum_h \Psi_{H/\delta}(h) \text{Kl}_3(\delta \alpha_1 h; r_1 s / (\delta, r_1 s)) \overline{\text{Kl}_3(\delta \alpha_2 h; r_2 s / (\delta, r_2 s))} \end{aligned}$$

for some $\alpha_i \in (\mathbb{Z}/r_i s / (\delta, r_i s) \mathbb{Z})^\times$. By Lemma 6.25 and Lemma 4.9, we have

$$S_1(\delta) \ll (s[r_1, r_2])^\varepsilon \left(\frac{H}{\delta s[r_1, r_2]} + 1 \right) \left(\frac{s[r_1, r_2]}{\delta} \right)^{1/2} (a_2 - a_1, r_1, r_2)^{1/2} (a_2 r_1^3 - a_1 r_2^3, s)^{1/2}$$

(the gcd factors for $S_1(\delta)$ are divisors of those for $\delta = 1$). Summing over $\delta \mid s[r_1, r_2]$ then gives the result. \square

6.10.3. The Katz Sato-Tate law over short intervals. In this section, which is independent of the rest of this paper, we give a sample application of the van der Corput method to Katz's equidistribution law for the angles of the Kloosterman sums $\text{Kl}_2(n; q)$.

Given a squarefree integer $q \geq 1$ with $\omega(q) \geq 1$ prime factors, we define the *Kloosterman angle* $\theta(n; q) \in [0, \pi]$ by the formula

$$2^{\omega(q)} \cos(\theta(n; q)) = \text{Kl}_2(n; q).$$

In [32], as a consequence of the determination of the geometric monodromy group of the Kloosterman sheaf \mathcal{Kl}_2 , Katz proved (among other things) a result which can be phrased as follows:

Theorem 6.27 (Katz's Sato-Tate equidistribution law). *As $p \rightarrow \infty$, the set of angles*

$$\{\theta(n; p), 1 \leq n \leq p\} \in [0, \pi]$$

becomes equidistributed in $[0, \pi]$ with respect to the Sato-Tate measure μ_{ST} with density

$$\frac{2}{\pi} \sin^2(\theta) d\theta,$$

i.e., for any continuous function $f : [0, \pi] \rightarrow \mathbb{C}$, we have

$$\int f(x) d\mu_{ST}(x) = \lim_{p \rightarrow +\infty} \frac{1}{p-1} \sum_{1 \leq n \leq p} f(\theta(n; p)).$$

By the Pólya-Vinogradov method one can reduce the length of the interval $[1, p]$:

Proposition 6.28. *For any $\varepsilon > 0$, the set of angles*

$$\{\theta(n; p), 1 \leq n \leq p^{1/2+\varepsilon}\} \in [0, \pi]$$

becomes equidistributed on $[0, \pi]$ with respect to the Sato-Tate measure μ_{ST} as $p \rightarrow +\infty$.

(In fact, using the “sliding sum method” [18], one can reduce the range to $1 \leq n \leq p^{1/2}\Psi(p)$ for any increasing function Ψ with $\Psi(p) \rightarrow +\infty$).

As we show here, as a very special example of application of the van der Corput method, we can prove a version of Katz's Sato-Tate law for Kloosterman sums of composite moduli over shorter ranges:

Theorem 6.29. *Let q denote integers of the form $q = rs$ where r, s are two distinct primes satisfying*

$$s^{1/2} \leq r \leq 2s^{1/2}.$$

For any $\varepsilon > 0$, the set of pairs of angles

$$\{(\theta(n\bar{s}^2; r), \theta(n\bar{r}^2; s)), 1 \leq n \leq q^{1/3+\varepsilon}\} \in [0, \pi]^2$$

becomes equidistributed on $[0, \pi]^2$ with respect to the product measure $\mu_{ST} \times \mu_{ST}$ as $q \rightarrow +\infty$ among such integers.

Consequently the set

$$\{\theta(n; q), 1 \leq n \leq q^{1/3+\varepsilon}\} \in [0, \pi]$$

becomes equidistributed on $[0, \pi]$ with respect to the measure $\mu_{ST,2}$ obtained as the push forward of the measure $\mu_{ST} \times \mu_{ST}$ by the map $(\theta, \theta') \mapsto \text{acos}(\cos \theta \cos \theta')$.

Proof. The continuous functions

$$\text{sym}_{k,k'}(\theta, \theta') := \text{sym}_k(\theta) \text{sym}_{k'}(\theta') = \frac{\sin((k+1)\theta)}{\sin \theta} \frac{\sin((k+1)\theta')}{\sin \theta'}$$

for $(k, k') \in \mathbb{N}_{\geq 0} - \{(0, 0)\}$ generate a dense subspace of the space of continuous functions on $[0, \pi]^2$ with mean 0 with respect to $\mu_{ST} \times \mu_{ST}$. Thus, by the classical Weyl criterion, it is enough to prove that

$$\sum_{1 \leq n \leq q^{1/3+\varepsilon}} \text{sym}_k(\theta(\bar{s}^2 n; r)) \text{sym}_{k'}(\theta(\bar{r}^2 n; s)) = o(q^{1/3+\varepsilon}).$$

By partition of unity, it is sufficient to prove that

$$\sum_n \Psi\left(\frac{n}{N}\right) \text{sym}_k(\theta(\bar{s}^2 n; r)) \text{sym}_{k'}(\theta(\bar{r}^2 n; s)) \ll_{k,k'} q^{1/3+9\varepsilon/10}. \quad (6.26)$$

for any $N \leq q^{1/3+\varepsilon} \log q$ and any smooth function Ψ as above, where the subscripting in $\ll_{k,k'}$ indicates that the implied constant is allowed to depend on k, k' . For any fixed (k, k') , the function

$$x \mapsto \text{sym}_{k'}(\theta(\bar{r}^2 x; s))$$

is a trace function modulo s , namely the trace function associated to the lisse sheaf obtained by composing the representation corresponding to the rank 2 pullback of the Kloosterman sheaf $[\times \bar{r}^2]^* \mathcal{K}\ell_2$ with the k^{th} symmetric power representation $\text{sym}_{k'} : \text{GL}_2 \rightarrow \text{GL}_{k'+1}$. By [32], this sheaf $\text{sym}_{k'} \mathcal{K}\ell_2$ is non-trivial if $k' \geq 1$, and geometrically irreducible of rank $k' + 1 > 1$. Therefore, if $k' \geq 1$, the van der Corput method (6.22) (see also Remark 6.22) gives

$$\sum_n \Psi_N(n) \text{sym}_k(\theta(\bar{s}^2 n; r)) \text{sym}_{k'}(\theta(\bar{r}^2 n; s)) \ll N^{1/2} q^{1/6} \ll_{k,k'} q^{1/3+9\varepsilon/10}.$$

Indeed, $\text{sym}_{k'} \mathcal{K}\ell_2$, being geometrically irreducible of rank > 1 , does not contain any quadratic phase.

If $k' = 0$ (so that the function modulo s is the constant function 1), then we have $k \geq 1$ and $\text{sym}_k \mathcal{K}\ell_2$ is geometrically irreducible of rank > 1 . Therefore it does not contain any linear phase, and by the Pólya-Vinogradov method (6.21), we deduce

$$\sum_n \Psi_N(n) \text{sym}_k(\theta(\bar{s}^2 n; r)) \text{sym}_{k'}(\theta(\bar{r}^2 n; s)) \ll r^{1/2+\eta} (1 + N/r) \ll_{\eta} q^{1/6+\eta+\varepsilon}$$

for any $\eta > 0$. □

7. THE TYPE III ESTIMATE

In this section we establish Theorem 2.8(v). Let us recall the statement:

Theorem 7.1 (New Type III estimates). *Let $\varpi, \delta, \sigma > 0$ be fixed quantities, let I be a bounded subset of \mathbb{R} , let $i \geq 1$ be fixed, let $a \pmod{P_1}$ be a primitive congruence class, and let $M, N_1, N_2, N_3 \gg 1$ be quantities with*

$$MN_1 N_2 N_3 \asymp x \quad (7.1)$$

$$N_1 N_2, N_1 N_3, N_2 N_3 \gg x^{1/2+\sigma} \quad (7.2)$$

$$x^{2\sigma} \ll N_1, N_2, N_3 \ll x^{1/2-\sigma}. \quad (7.3)$$

Let $\alpha, \psi_1, \psi_2, \psi_3$ be smooth coefficient sequences located at scales M, N_1, N_2, N_3 , respectively. Then we have the estimate

$$\sum_{\substack{d \in \mathcal{D}_I(x^\delta) \\ d \ll x^{1/2+2\varpi}}} |\Delta(\alpha \star \psi_1 \star \psi_2 \star \psi_3; a(d))| \ll x \log^{-A} x$$

for any fixed $A > 0$, provided that

$$\varpi < \frac{1}{12}, \quad \sigma > \frac{1}{18} + \frac{28}{9}\varpi + \frac{2}{9}\delta. \quad (7.4)$$

Our proof of this theorem is inspired in part by the recent work of Fouvry, Kowalski and Michel [16], in which the value of the exponent of distribution of the ternary divisor function $\tau_3(n)$ in arithmetic progressions to large (prime) moduli is improved upon the earlier results of Friedlander-Iwaniec [14] and Heath-Brown [27]. Our presentation is also more streamlined. The present argument moreover exploits the existence of an averaging over divisible moduli to derive further improvements to the exponent.

7.1. Sketch of proofs. Before we give the rigorous argument, let us first sketch the solution of the model problem (in the spirit of Section 5.2), of obtaining a non-trivial estimate for

$$\sum_{q \asymp Q} |\Delta(\psi_1 \star \psi_2 \star \psi_3, a(q))| \quad (7.5)$$

for Q slightly larger than $x^{1/2}$ in logarithmic scale (i.e. out of reach of the Bombieri-Vinogradov theorem). Here ψ_1, ψ_2, ψ_3 are smooth coefficient sequences at scales N_1, N_2, N_3 respectively with $N_1 N_2 N_3 \asymp x$ and $N_1, N_2, N_3 \ll \sqrt{x}$, and q is implicitly restricted to suitably smooth or densely divisible moduli (we do not make this precise to simplify the exposition). The trivial bound for this sum is $\ll \log^{O(1)} x$, and we wish to improve it at least by a factor $\log^{-A} x$ for arbitrary fixed $A > 0$.

This problem is equivalent to that of estimating

$$\sum_{q \asymp Q} c_q \Delta(\psi_1 \star \psi_2 \star \psi_3, a(q))$$

when c_q is an arbitrary bounded sequence. As in Section 5.2, we write EMT for unspecified main terms, and we wish to control the expression

$$\sum_{q \asymp Q} c_q \sum_{n=a(q)} \psi_1 \star \psi_2 \star \psi_3(n) - \text{EMT}$$

to accuracy better than x . After expanding the convolution and completing the sums, this sum can be transformed to a sum roughly of the form

$$\frac{1}{H} \sum_{1 \leq |h_i| \leq H_i} \sum_{q \asymp Q} c_q \sum_{\substack{n_1, n_2, n_3 \in \mathbb{Z}/q\mathbb{Z} \\ n_1 n_2 n_3 = a(q)}} e_q(h_1 n_1 + h_2 n_2 + h_3 n_3)$$

where $H_i := Q/N_i$ and $H := H_1 H_2 H_3 \asymp Q^3/x$, the main term having cancelled out with the zero frequencies. As we are taking Q close to $x^{1/2}$, H is thus close to $x^{1/2}$ as well. Ignoring the degenerate cases when h_1, h_2, h_3 share a common factor with q , we

see from (6.20) that

$$\sum_{\substack{n_1, n_2, n_3 \in \mathbb{Z}/q\mathbb{Z} \\ n_1 n_2 n_3 = a \pmod{q}}} e_q(h_1 n_1 + h_2 n_2 + h_3 n_3) = q \text{Kl}_3(ah_1 h_2 h_3; q),$$

so we are now dealing essentially with the sum of hyper-Kloosterman sums

$$\frac{Q}{H} \sum_{1 \leq |h_i| \ll H_i} \sum_{q \asymp Q} c_q \text{Kl}_3(ah_1 h_2 h_3; q) = \frac{Q}{H} \sum_{1 \leq |h| \ll H} \tilde{\tau}_3(h) \sum_{q \asymp Q} c_q \text{Kl}_3(ah; q)$$

where

$$\tilde{\tau}_3(h) := \sum_{\substack{1 \leq |h_i| \ll H_i \\ h_1 h_2 h_3 = h}} 1$$

is a variant of the divisor function τ_3 .

A direct application of the deep Deligne bound

$$|\text{Kl}_3(ah; q)| \ll 1 \tag{7.6}$$

for hyper-Kloosterman sums (see Remark 6.10) gives the trivial bound $\ll Q^2$, which just fails to give the desired result, so the issue is to find some extra cancellation in the phases of the hyper-Kloosterman sums.

One can apply immediately the Cauchy-Schwarz inequality to eliminate the weight $\tilde{\tau}_3(h)$, but it turns out to be more efficient to first use the assumption that q is restricted to densely divisible moduli and to factor $q = rs$ where $r \asymp R$, $s \asymp S$, in which R and S are well-chosen in order to balance the diagonal and off-diagonal components resulting from the Cauchy-Schwarz inequality (it turns out that the optimal choices here will be $R, S \approx x^{1/4}$).

Applying this factorization, and arguing for each s separately, we are led to expressions of the form

$$\frac{Q}{H} \sum_{1 \leq |h| \ll H} \tilde{\tau}_3(h) \sum_{r \asymp R} c_{rs} \text{Kl}_3(ah; rs),$$

where we must improve on the bound $\ll QR$ coming from (7.6) for any given $s \asymp S$. If we then apply the Cauchy-Schwarz inequality to the sum over h , we get

$$\begin{aligned} \frac{Q}{H} \sum_{1 \leq |h| \ll H} \tilde{\tau}_3(h) \sum_{r \asymp R} c_{rs} \text{Kl}_3(ah; rs) &\ll \frac{Q}{H^{1/2}} \left(\sum_{1 \leq |h| \ll H} \left| \sum_{r \asymp R} c_{rs} \text{Kl}_3(ah; rs) \right|^2 \right)^{1/2} \\ &\ll \frac{Q}{H^{1/2}} \left(\sum_{r_1, r_2 \asymp R} \sum_{1 \leq |h| \ll H} \text{Kl}_3(ah; r_1 s) \overline{\text{Kl}_3(ah; r_2 s)} \right)^{1/2}. \end{aligned}$$

The inner sum over h is now essentially of the type considered by Corollary 6.26, and this result gives an adequate bound. Indeed, the contribution of the diagonal terms $r_1 = r_2$ is $\ll RH$ (using (7.6)) and the contribution of each non-diagonal sum (assuming we are in the model case where r_1, r_2 are coprime, and the other greatest common divisors appearing in Corollary 6.26 are negligible) is

$$\sum_{1 \leq |h| \ll H} \text{Kl}_3(ah; r_1 s) \overline{\text{Kl}_3(ah; r_1 s)} \ll (r_1 r_2 s)^{1/2} \ll RS^{1/2}$$

by Corollary 6.26, leading to a total estimate of size

$$\ll \frac{Q}{H^{1/2}} \left(R^{1/2} H^{1/2} + R^{3/2} S^{1/4} \right).$$

If $R = S \approx x^{1/4}$, this is very comfortably better than what we want, and this strongly suggests that we can take Q quite a bit larger than $x^{1/2}$.

Remark 7.2. It is instructive to run the same analysis for the fourth order sum

$$\sum_{q \asymp Q} |\Delta(\psi_1 \star \psi_2 \star \psi_3 \star \psi_4, a(q))|$$

where $\psi_1, \psi_2, \psi_3, \psi_4$ are smooth at scales N_1, N_2, N_3, N_4 with $N_1 \dots N_4 \asymp x$ and $N_1, \dots, N_4 \ll x^{1/2} \approx Q$. This is a model for the “Type IV” sums mentioned in Remark 3.2, and is clearly related to the exponent of distribution for the divisor function τ_4 .

The quantity H is now of the form $H \approx Q^4/x \approx x$, and one now has to estimate the sum

$$\sum_{1 \leq |h| \leq H} \tilde{\tau}_4(h) \sum_{q \asymp Q} c_q \text{Kl}_4(ah; q)$$

to accuracy better than $Hx/Q^{3/2} \approx x^{5/4}$. If we apply the Cauchy-Schwarz inequality in the same manner after exploiting a factorization $q = rs$ with $r \asymp R$, $s \asymp S$ and $RS \asymp Q \approx x^{1/2}$, we end up having to control

$$\sum_{r_1, r_2 \asymp R} \sum_{1 \leq |h| \leq H} \left| \sum_{1 \leq |h| \leq H} \text{Kl}_4(ah; r_1 s) \overline{\text{Kl}_4(ah; r_2 s)} \right|$$

with accuracy better than $(x^{5/4}/S)^2/H \approx x^{3/2}/S^2$. The diagonal contribution $r_1 = r_2$ is $\ll RH \approx x^{3/2}/S$, and the off-diagonal contribution is $\approx R^2(R^2S)^{1/2} \approx x^{3/2}/S^{5/2}$. However even with the optimal splitting $S \approx 1$, $R \approx Q$, one cannot make both of these terms much smaller than the target accuracy of $x^{3/2}/S^2$. Thus the above argument does not improve upon the Bombieri-Vinogradov inequality for Type IV sums. (It is known, due to Linnik, that the exponent of distribution for τ_4 is at least $1/2$, in the stronger sense that the asymptotic formula holds for all moduli $\leq x^{1/2-\varepsilon}$ for $\varepsilon > 0$.) The situation is even worse, as the reader will check, for the Type V sums, in that one now cannot even recover Bombieri-Vinogradov with this method.

We will give the rigorous proof of Theorem 2.8(v) in the next two sections, by first performing the reduction to exponential sums, and then concluding the proof.

7.2. Reduction to exponential sums. By Theorem 2.9 (the general version of the Bombieri-Vinogradov theorem) we have

$$\sum_{q \leq x^{1/2} \log^{-B(A)} x} |\Delta(\alpha \star \psi_1 \star \psi_2 \star \psi_3)| \ll x \log^{-A} x$$

for some $B(A) \geq 0$. We may therefore restrict our attention to moduli q in the range $x^{1/2}/\log^B x \leq q \ll x^{1/2+2\varpi}$.

We also write $N = N_1 N_2 N_3$. From (7.2) and (7.3), we deduce

$$x^{3/4+3\sigma/2} \ll (N_1 N_2)^{1/2} (N_1 N_3)^{1/2} (N_2 N_3)^{1/2} = N \ll x^{3/2-3\sigma}. \quad (7.7)$$

It is convenient to restrict q to a finer-than-dyadic interval $\mathcal{I}(Q)$ in order to separate variables later using Taylor expansions. More precisely, for a small fixed $\varepsilon > 0$ and some fixed $c \geq 1$, we denote by $\mathcal{I} = \mathcal{I}(Q)$ a finer-than-dyadic interval of the type

$$\mathcal{I}(Q) := \{q : Q(1 - cx^{-\varepsilon}) \leq q \leq Q(1 + cx^{-\varepsilon})\},$$

(assuming, as always, that x is large, so that $cx^{-\varepsilon}$ is less than (say) $1/2$) and abbreviate

$$\sum_q A_q = \sum_{\substack{q \in \mathcal{D}_I(x^\delta) \\ q \in \mathcal{I}(Q)}} A_q$$

for any A_q .

Theorem 7.1 will clearly follow if we prove that, for $\varepsilon > 0$ sufficiently small, we have

$$\sum_q |\Delta(\alpha \star \psi_1 \star \psi_2 \star \psi_3; a(q))| \ll x^{-2\varepsilon} MN \quad (7.8)$$

for all Q such that

$$x^{1/2} \ll Q \ll x^{1/2+2\varpi}. \quad (7.9)$$

We fix Q as above and denote by $\Sigma(Q; a)$ the left-hand side of (7.8). We have

$$\Sigma(Q; a) = \sum_q c_q \Delta(\alpha \star \psi_1 \star \psi_2 \star \psi_3; a(q))$$

for some sequence c_q with $|c_q| = 1$. We will prove that, for any $a(q)$, we have

$$\sum_q c_q \sum_{n=a(q)} (\alpha \star \psi_1 \star \psi_2 \star \psi_3)(n) = X + O(x^{-2\varepsilon+o(1)} MN) \quad (7.10)$$

for some X that is independent of a (but that can depend on all other quantities, such as c_q , α , or ψ_1, ψ_2, ψ_3). Then (7.8) follows by averaging over all a coprime to P_I (as in the reduction to (5.18) in Section 5).

The left-hand side of (7.10), say $\Sigma_1(Q; a)$, is equal to

$$\Sigma_1(Q; a) = \sum_q c_q \sum_{(m,q)=1} \alpha(m) \sum_{n_1, n_2, n_3} \psi_1(n_1) \psi_2(n_2) \psi_3(n_3) \mathbf{1}_{mn_1 n_2 n_3 = a(q)}. \quad (7.11)$$

The next step is a variant of the completion of sums technique from Lemma 4.9. In that lemma, the Fourier coefficients of the cutoff functions were estimated individually using the fast decay of the Fourier transforms. In our current context, we want to keep track to some extent of their dependency on the variable q . Since we have restricted q to a rather short interval, we can separate the variables fairly easily using a Taylor expansion.

Note first that for $i = 1, 2, 3$, one has

$$N_i \ll x^{1/2-\sigma} \ll x^{-\sigma} Q,$$

so in particular ψ_i is supported in $(-q/2, q/2]$ if x is large enough. By discrete Fourier inversion, we have

$$\psi_i(x) = \frac{1}{q} \sum_{-q/2 < h \leq q/2} \Psi_i\left(\frac{h}{q}\right) e\left(\frac{hx}{q}\right) \quad (7.12)$$

where

$$\Psi_i(y) = \sum_n \psi_i(n) e(-ny)$$

is the analogue of the function Ψ in the proof of Lemma 4.9. As in that lemma, using the smoothness of ψ_i , Poisson summation, and integration by parts, we derive the bound

$$|\Psi_i(y)| \ll N_i(1 + N_i|y|)^{-C}$$

for any fixed $C \geq 0$ and any $-1/2 \leq y \leq 1/2$ (see (4.17)). More generally we obtain

$$|\Psi_i^{(j)}(y)| \ll N_i^{1+j}(1 + N_i|y|)^{-C}$$

for any fixed $C \geq 0$, any $j \geq 0$ and any $-1/2 \leq y \leq 1/2$.

Denoting $H_i := Q/N_i \gg x^\sigma$, we thus have

$$\Psi_i^{(j)}\left(\frac{h}{q}\right) \ll x^{-100}$$

(say) for $x^{\varepsilon/2}H_i < |h| \leq q/2$ and all fixed j . On the other hand, for $|h| \leq x^{\varepsilon/2}H_i$ and $q \in \mathcal{I}$, a Taylor expansion using the definition of \mathcal{I} and H_i gives

$$\frac{1}{q}\Psi_i\left(\frac{h}{q}\right) = \frac{1}{q} \sum_{j=0}^J \frac{1}{j!} \Psi_i^{(j)}(h/Q) \eta^j + O(N_i^{2+J}|\eta|^{J+1})$$

for any fixed J where α is the q -dependent quantity

$$\eta := \frac{h}{q} - \frac{h}{Q} = \frac{h(Q-q)}{qQ} \ll x^{-\varepsilon} \frac{h}{Q} \ll x^{-\varepsilon/2} \frac{1}{N_i}.$$

Thus we obtain

$$\frac{1}{q}\Psi_i\left(\frac{h}{q}\right) = \frac{1}{q} \sum_{j=0}^J \frac{1}{j!} \Psi_i^{(j)}\left(\frac{h}{Q}\right) \left(\frac{h}{Q}\right)^j \left(\frac{q-Q}{q}\right)^j + O(x^{-(J+1)\varepsilon/2} N_i).$$

Taking J large enough, depending on $\varepsilon > 0$ but still fixed, this gives an expansion

$$\frac{1}{q}\Psi_i\left(\frac{h}{q}\right) = 1_{|h| < x^{\varepsilon/2}H_i} \frac{1}{H_i} \sum_{j=0}^J c_i(j, h) \frac{Q}{q} \left(\frac{q-Q}{q}\right)^j + O(x^{-100}) \quad (7.13)$$

with coefficients that satisfy

$$c_i(j, h) = \frac{1}{j!} \Psi_i^{(j)}\left(\frac{h}{Q}\right) \left(\frac{h}{Q}\right)^j \frac{H_i}{Q} \ll 1,$$

as well as

$$\left(\frac{Q}{q}\right) \left(\frac{q-Q}{q}\right)^j \ll 1.$$

Let

$$H := H_1 H_2 H_3 = Q^3/N. \quad (7.14)$$

Inserting (7.13) for $i = 1, 2, 3$ into (7.12) and the definition (7.11) of $\Sigma_1(Q; a)$, we see that $\Sigma_1(Q; a)$ can be expressed (up to errors of $O(x^{-100})$) as a sum of a bounded number (depending on ε) of expressions, each of the form

$$\Sigma_2(Q; a) = \frac{1}{H} \sum_q \eta_q \sum_{(m, q)=1} \alpha(m) \sum_{\mathbf{h}} c(\mathbf{h}) \sum_{\mathbf{n} \in (\mathbb{Z}/q\mathbb{Z})^3} e_q(h_1 n_1 + h_2 n_2 + h_3 n_3) \mathbf{1}_{mn_1 n_2 n_3 = a \pmod{q}},$$

where η_q is a bounded sequence supported on $\mathcal{I} \cap \mathcal{D}_I(x^\delta)$, $\mathbf{h} := (h_1, h_2, h_3)$ and $c(\mathbf{h})$ are bounded coefficients supported on $|h_i| \leq x^{\varepsilon/2} H_i$, and \mathbf{n} abbreviates (n_1, n_2, n_3) . Our task is now to show that

$$\Sigma_2(Q; a) = X_2 + O(x^{-2\varepsilon+o(1)} MN)$$

for some quantity X_2 that can depend on quantities such as η_q , α , c , H , but which is independent of a .

We use $F(\mathbf{h}, a; q)$ to denote the hyper-Kloosterman type sum

$$F(\mathbf{h}, a; q) := \frac{1}{q} \sum_{\mathbf{n} \in ((\mathbb{Z}/q\mathbb{Z})^\times)^3} e_q(h_1 n_1 + h_2 n_2 + h_3 n_3) \mathbf{1}_{n_1 n_2 n_3 = a \pmod{q}} \quad (7.15)$$

for $\mathbf{h} = (h_1, h_2, h_3) \in (\mathbb{Z}/q\mathbb{Z})^3$ and $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ (note that the constraint $n_1 n_2 n_3 = a \pmod{q}$ forces n_1, n_2, n_3 coprime to q), so that

$$\Sigma_2(Q; a) = \frac{Q}{H} \sum_q \eta'_q \sum_{(m, q)=1} \alpha(m) \sum_{\mathbf{h}} c(\mathbf{h}) F(\mathbf{h}, a\overline{m}; q)$$

where $\eta'_q := \frac{q}{Q} \eta_q$ is a slight variant of η_q .

We next observe that $F(\mathbf{h}, a\overline{m}; q)$ is independent of a if $h_1 h_2 h_3 = 0$ (as can be seen by a change of variable). Thus the contribution X_2 to the sum from tuples \mathbf{h} with $h_1 h_2 h_3 = 0$ is independent of a . The combination of these terms X_2 in the decomposition of $\Sigma_1(Q; a)$ in terms of instances of $\Sigma_2(Q; a)$ is the quantity X in (7.10). We denote by $\Sigma'_2(Q; a)$ the remaining contribution. Our task is now to show that

$$\Sigma'_2(Q, a) \ll x^{-2\varepsilon} MN. \quad (7.16)$$

We must handle possible common factors of q and $h_1 h_2 h_3$ for $h_1 h_2 h_3 \neq 0$ (the reader may skip the necessary technical details and read on while assuming that q is always coprime to each of the h_i , so that all the b -factors appearing below become equal to 1).

For $i = 1, 2, 3$, we write

$$h_i = b_i l_i$$

where $(l_i, q) = 1$ and $b_i \mid q^\infty$ (i.e., b_i is the product of all the primes in h_i , with multiplicity, that also divide q). We also write

$$b := \prod_{p \mid b_1 b_2 b_3} p = (h_1 h_2 h_3, q), \quad (7.17)$$

so that we have a factorization $q = bd$, where $d \in \mathcal{D}_I(bx^\delta)$ by Lemma 2.10(i), since q is x^δ -densely divisible.

By Lemma 4.4, we have

$$F(\mathbf{h}, a\overline{m}; q) = F(\overline{d}\mathbf{h}, a\overline{m}; b) F(\overline{b}\mathbf{h}, a\overline{m}; d)$$

where $\overline{b}\mathbf{h} := (\overline{b}h_1, \overline{b}h_2, \overline{b}h_3)$. By an easy change of variable, the second factor satisfies

$$F(\overline{b}\mathbf{h}, a\overline{m}; d) = \text{Kl}_3(ah_1 h_2 h_3 \overline{mb^3}; d) = \text{Kl}_3\left(\frac{ab_1 b_2 b_3 l_1 l_2 l_3}{b^3} \frac{1}{m}; d\right).$$

We observe that the residue class $ab_1 b_2 b_3 \overline{mb^3} \pmod{d}$ is invertible.

Denoting $\mathbf{b} := (b_1, b_2, b_3)$, $\mathbf{l} := (l_1, l_2, l_3)$, we can thus write

$$\Sigma'_2(Q; a) = \frac{Q}{H} \sum_{\mathbf{b}} \sum_{\mathbf{l}} c(\mathbf{b}, \mathbf{l}) \sum_{\substack{d \in \mathcal{D}_I(bx^\delta) \\ (d, bl_1 l_2 l_3) = 1}} \eta'_{bd} \sum_{(m, bd) = 1} \alpha(m) F(\bar{d}\mathbf{h}, a\bar{m}; b) \text{Kl}_3\left(\frac{ab_1 b_2 b_3}{b^3} \frac{l_1 l_2 l_3}{m}; d\right)$$

where b is defined as in (7.17), $c(\mathbf{b}, \mathbf{l}) := c(b_1 l_1, b_2 l_2, b_3 l_3)$, and the sum over l_i is now over the range

$$0 < |l_i| \leq \frac{x^{\varepsilon/2} H_i}{b_i}. \quad (7.18)$$

To control the remaining factor of F , we have the following estimate, where we denote by n^\flat the largest squarefree divisor of an integer $n \geq 1$ (the *squarefree radical* of n). Note that $b = (b_1 b_2 b_3)^\flat$.

Lemma 7.3. *Let the notation and hypotheses be as above.*

(1) *We have*

$$|F(\bar{d}\mathbf{h}, a\bar{m}; b)| \leq \frac{b_1^\flat b_2^\flat b_3^\flat}{b^2}.$$

(2) *The sum $F(\bar{d}\mathbf{h}, a\bar{m}; b)$ is independent of d and m .*

Proof. By further applications of Lemma 4.4 it suffices for (1) to show that

$$|F(\mathbf{c}, a; p)| \leq \frac{(c_1, p)(c_2, p)(c_3, p)}{p^2}$$

whenever p is prime, $\mathbf{c} = (c_1, c_2, c_3) \in (\mathbb{Z}/p\mathbb{Z})^3$, with $c_1 c_2 c_3 = 0 \pmod{p}$, and $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Without loss of generality we may assume that $c_3 = 0 \pmod{p}$, and then

$$F(\mathbf{c}, a; p) = \frac{1}{p} \sum_{n_1, n_2 \in (\mathbb{Z}/p\mathbb{Z})^\times} e_p(c_1 n_1 + c_2 n_2),$$

from which the result follows by direct computation of Ramanujan sums (see e.g. [30, (3.5)]). Similarly, we see that the value of $F(\mathbf{c}, a; p)$ only depends on which c_i are divisible by p and which are not, and this gives (2). \square

This lemma leads to the estimate

$$\begin{aligned} |\Sigma'_2(Q; a)| &\ll \frac{Q}{H} \sum_{\mathbf{b}} \frac{b_1^\flat b_2^\flat b_3^\flat}{b^2} \sum_{\mathbf{l}} \left| \sum_{\substack{d \in \mathcal{D}_I(bx^\delta) \\ (bl_1 l_2 l_3, d) = 1}} \eta'_{bd} \sum_{(m, bd) = 1} \alpha(m) \text{Kl}_3\left(\frac{ab_1 b_2 b_3 l_1 l_2 l_3}{b^3 m}; d\right) \right| \\ &\ll \frac{Q}{H} \sum_{\mathbf{b}} \frac{b_1^\flat b_2^\flat b_3^\flat}{b^2} T(\mathbf{b}) \end{aligned} \quad (7.19)$$

with

$$T(\mathbf{b}) := \sum_{0 < |\ell| \leq x^{3\varepsilon/2} H / b_1 b_2 b_3} \tau_3(\ell) \left| \sum_{\substack{d \in b^{-1} \mathcal{D}_I(bx^\delta) \cap \mathcal{I} \\ (b\ell, d) = 1}} \eta'_{bd} \sum_{(m, bd) = 1} \alpha(m) \text{Kl}_3\left(\frac{a\ell b_1 b_2 b_3}{b^3 m}; d\right) \right|;$$

following [27] (particularly the arguments on p. 42), we have collected common values of $\ell = l_1 l_2 l_3$, and also replaced the bounded coefficients η'_{bd} , supported on \mathcal{I} , with their absolute values. This is the desired reduction of Type III estimates to exponential sums.

7.3. End of the proof. We now focus on estimating $T(\mathbf{b})$. First of all, we may assume that

$$\frac{Q}{b} \gg 1, \quad x^{3\varepsilon/2} \frac{H}{b_1 b_2 b_3} \gg 1 \quad (7.20)$$

since otherwise $T(\mathbf{b}) = 0$.

Let $y = bx^\delta$ and let S be a parameter such that

$$1 \leq S \leq y \frac{Q}{2b} = \frac{x^\delta Q}{2}. \quad (7.21)$$

The moduli d in the definition of $T(\mathbf{b})$ are y -densely divisible and we have $1 \leq S \leq dy$ (for x sufficiently large), so that there exists a factorization $d = rs$ with

$$y^{-1}S \leq s \leq S, \quad \frac{Q}{bS} \ll r \ll \frac{yQ}{bS},$$

and $(r, s) = 1$ (if $d < S \leq dy$, we take $s = d$ and $r = 1$).

Thus we may write

$$T(\mathbf{b}) \ll \sum_{\substack{y^{-1}S \leq s \leq S \\ (b\ell, s)=1}} \sum_{0 < |\ell| \leq H_{\mathbf{b}}} \tau_3(\ell) \left| \sum_{\substack{r \in \mathcal{S}_I \\ \frac{Q}{bS} \ll r \ll \frac{yQ}{bS} \\ (b\ell s, r)=1}} \eta'_{b,r,s} \sum_{(m, brs)=1} \alpha(m) \text{Kl}_3\left(\frac{a\ell b_1 b_2 b_3}{b^3 m}; rs\right) \right|$$

where $\eta'_{b,r,s}$ is some bounded sequence and

$$H_{\mathbf{b}} := \frac{x^{3\varepsilon/2} H}{b_1 b_2 b_3}.$$

We apply the Cauchy-Schwarz inequality to the sum over s and ℓ . As usual, we may insert a smooth coefficient sequence $\psi_{H_{\mathbf{b}}}$ at scale $H_{\mathbf{b}}$, equal to one on $[-H_{\mathbf{b}}, H_{\mathbf{b}}]$, and derive

$$|T(\mathbf{b})|^2 \leq T_1 T_2$$

where

$$T_1 := \sum_{y^{-1}S \leq s \leq S} \frac{1}{s} \sum_{0 < |\ell| \leq H_{\mathbf{b}}} \tau_3(\ell)^2 \ll H_{\mathbf{b}}$$

(by Lemma 1.2) and

$$T_2 := \sum_{y^{-1}S \leq s \leq S} \sum_{\ell} s \psi_{H_{\mathbf{b}}}(\ell) \left| \sum_{\substack{r \in \mathcal{S}_I \\ \frac{Q}{bS} \ll r \ll \frac{yQ}{bS} \\ (b\ell, rs)=(r,s)=1}} \eta'_{b,r,s} \sum_{(m, brs)=1} \alpha(m) \text{Kl}_3\left(\frac{a\ell b_1 b_2 b_3}{b^3 m}; rs\right) \right|^2.$$

We expand the square and find

$$|T_2| \leq \sum_{y^{-1}S \leq s \leq S} s \sum_{r_1, r_2} \sum_{m_1, m_2} |\alpha(m_1)| |\alpha(m_2)| |U(r_1, r_2, s, m_1, m_2)|,$$

where we have omitted the summation conditions

$$r_i \in \mathcal{S}_I; \frac{Q}{bS} \ll r_i \ll \frac{yQ}{bS}; (b\ell, r_i s) = (r_i, s) = (m_i, br_i s) = 1 \text{ for } i = 1, 2$$

on r_1, r_2 and m_1, m_2 for brevity, and where

$$U(r_1, r_2, s, m_1, m_2) := \sum_{\ell: (\ell, r_1 r_2 s)=1} \psi_{H_{\mathbf{b}}}(\ell) \text{Kl}_3\left(\frac{a\ell b_1 b_2 b_3}{b^3 m_1}; r_1 s\right) \overline{\text{Kl}_3\left(\frac{a\ell b_1 b_2 b_3}{b^3 m_2}; r_2 s\right)}$$

is exactly the type of sum considered in Corollary 6.26 (recall that $ab_1b_2b_3$ is coprime to r_1r_2s).

We first consider the “diagonal terms”, which here mean the cases where

$$\frac{ab_1b_2b_3}{b^3m_1}r_2^3 - \frac{ab_1b_2b_3}{b^3m_2}r_1^3 = \frac{ab_1b_2b_3}{b^3m_1m_2}(m_2r_2^3 - m_1r_1^3) = 0.$$

Using the Deligne bound $|\text{Kl}_3(x; d)| \ll 1$ when $(d, x) = 1$ (Remark 6.10), this contribution T'_2 is bounded by

$$\begin{aligned} T'_2 &\ll H_b \sum_{r_1, r_2} \sum_{y^{-1}S \leq s \leq S} s \sum_{\substack{m_1, m_2 \\ m_1r_1^3 = m_2r_2^3}} |\alpha(m_1)\alpha(m_2)| \\ &\ll H_b M \sum_{Q/(bS) \ll r_1 \ll yQ/(bS)} \left(\frac{Q}{br_1}\right)^2 \end{aligned}$$

since each pair (r_1, m_1) determines $\ll 1$ pairs (r_2, m_2) , and since s is, for each r_1 , constrained to be $\asymp Q/(br_1)$ by the condition $r_1s \asymp Q/b$. Summing, we obtain

$$T'_2 \ll \frac{H_b M Q S}{b}. \quad (7.22)$$

We now turn to the off-diagonal case $m_1r_1^3 - m_2r_2^3 \neq 0$. By Corollary 6.26, we have

$$\begin{aligned} U(r_1, r_2, s, m_1, m_2) &\ll \left(\frac{H_b}{[r_1, r_2]_s} + 1\right) (s[r_1, r_2])^{1/2} \\ &\quad \times (r_1, r_2, m_2 - m_1)^{1/2} (m_1r_1^3 - m_2r_2^3, s)^{1/2} \end{aligned}$$

in this case. We now sum these bounds to estimate the non-diagonal contribution T''_2 to T_2 . This is a straightforward, if a bit lengthy, computation, and we state the result first:

Lemma 7.4. *We have*

$$T''_2 \ll \frac{M^2 Q^2}{b^2} \left(\frac{H_b b^{1/2}}{Q^{1/2}} \left(\frac{bS}{Q}\right)^{1/2} + \frac{Q^{1/2}}{b^{1/2}} \left(\frac{x^\delta Q}{S}\right)^{1/2} \right).$$

We first finish the proof of the Type III estimate using this. We first derive

$$T_2 = T'_2 + T''_2 \ll \frac{M Q H_b S}{b} + \frac{M^2 Q S^{1/2} H_b}{b} + \frac{y^{1/2} M^2 Q^3}{b^3 S^{1/2}}.$$

We select the parameter S now, by optimizing it to minimize the sum of the first and last terms, subject to the constraint $S \leq (yQ)/(2b)$. Precisely, let

$$S = \min\left(\left(\frac{Q}{b}\right)^{4/3} \frac{y^{1/3} M^{2/3}}{H_b^{2/3}}, \frac{yQ}{2b}\right).$$

This satisfies (7.21) if x is large enough: we have $S \leq (yQ)/(2b)$ by construction, while $S \geq 1$ (for x large enough) follows either from $(yQ)/(2b) \gg y/2$ (see (7.20)), or from

$$\left(\frac{Q}{b}\right)^4 \frac{y M^2}{H_b^2} = \frac{(b_1 b_2 b_3)^2}{b^2} \frac{(MN)^2 x^{\delta-3\varepsilon}}{b Q^2} \gg x^{2+\delta-3\varepsilon} Q^{-3} \gg x^{1/2+\delta-6\varpi-3\varepsilon} \gg x^\varepsilon$$

if $\varepsilon > 0$ is small enough (using $b \ll Q$ and $\varpi < 1/12$).

This value of S leads to

$$|T(\mathbf{b})|^2 \ll H_{\mathbf{b}} \left(\frac{y^{1/3} H_{\mathbf{b}}^{1/3} M^{5/3} Q^{7/3}}{b^{7/3}} + \frac{y^{1/6} H_{\mathbf{b}}^{2/3} M^{7/3} Q^{5/3}}{b^{5/3}} + M^2 \left(\frac{Q}{b} \right)^{5/2} \right)$$

(where the third term only arises if $S = (yQ)/(2b)$), which gives

$$T(\mathbf{b}) \ll \frac{x^{5\varepsilon/4}}{(b_1 b_2 b_3)^{1/2} b} \left(x^{\delta/6} H^{2/3} M^{5/6} Q^{7/6} + x^{\delta/12} H^{5/6} M^{7/6} Q^{5/6} + H^{1/2} M Q^{5/4} \right)$$

using the definition of $H_{\mathbf{b}}$ and the bound $b_i \geq 1$ (to uniformize the three denominators involving b and \mathbf{b}).

We will shortly establish the following elementary fact.

Lemma 7.5. *The unsigned series*

$$\sum_{b_1, b_2, b_3 \geq 1} \sum \sum \frac{b_1^b b_2^b b_3^b}{(b_1 b_2 b_3)^{1/2} b^3}$$

converges to a finite value.

Now from (7.19) and this lemma, we get

$$\Sigma'_2(Q; a) \ll \frac{x^{5\varepsilon/4} Q}{H} \left(x^{\delta/6} H^{2/3} M^{5/6} Q^{7/6} + x^{\delta/12} H^{5/6} M^{7/6} Q^{5/6} + H^{1/2} M Q^{5/4} \right),$$

We now show that this implies (7.16) under suitable conditions on δ , ϖ and σ . Indeed, we have

$$\frac{x^{5\varepsilon/4} Q}{H} \left(x^{\delta/6} H^{2/3} M^{5/6} Q^{7/6} + x^{\delta/12} H^{5/6} M^{7/6} Q^{5/6} + H^{1/2} M Q^{5/4} \right) \ll MN(E_1 + E_2 + E_3)$$

where

$$\begin{aligned} E_1 &:= \frac{x^{5\varepsilon/4+\delta/6} Q^{13/6}}{H^{1/3} M^{1/6} N} = \frac{x^{5\varepsilon/4+\delta/6-1/6} Q^{7/6}}{N^{1/2}} \ll Q^{7/6} x^{5\varepsilon/4+\delta/6-3\sigma/4-13/24} \\ E_2 &:= \frac{x^{5\varepsilon/4+\delta/12} Q^{11/6} M^{7/6}}{H^{1/6} M N} = \frac{x^{5\varepsilon/4+\delta/12+1/6} Q^{4/3}}{N} \ll Q^{4/3} x^{5\varepsilon/4+\delta/12-3\sigma/2-7/12} \\ E_3 &:= \frac{x^{5\varepsilon/4} Q^{9/4}}{H^{1/2} N} = \frac{x^{5\varepsilon/4} Q^{3/4}}{N^{1/2}} \ll Q^{3/4} x^{5\varepsilon/4-3/8-3\sigma/4} \end{aligned}$$

using the definition (7.14) of H and the lower bound (7.7) for N . Using $Q \ll x^{1/2+2\varpi}$, we see that we will have $E_1 + E_2 + E_3 \ll x^{-2\varepsilon}$ for some small positive $\varepsilon > 0$ provided

$$\begin{cases} \frac{7}{6}(\frac{1}{2} + 2\varpi) + \frac{\delta}{6} - \frac{3\sigma}{4} - \frac{13}{24} < 0 \\ \frac{4}{3}(\frac{1}{2} + 2\varpi) + \frac{\delta}{12} - \frac{3\sigma}{2} - \frac{7}{12} < 0 \\ \frac{3}{4}(\frac{1}{2} + 2\varpi) - \frac{3\sigma}{4} - \frac{3}{8} < 0 \end{cases} \Leftrightarrow \begin{cases} \sigma > \frac{28}{9}\varpi + \frac{2}{9}\delta + \frac{1}{18} \\ \sigma > \frac{16}{9}\varpi + \frac{1}{18}\delta + \frac{1}{18} \\ \sigma > 2\varpi. \end{cases}$$

However, the first condition implies the second and third. Thus we deduce Theorem 7.1, provided that we prove the two lemmas above, which we will now do.

Proof of Lemma 7.4. We will relax somewhat the conditions on r_1 , r_2 and s . We recall first that

$$\frac{Q}{bS} \ll r_1, r_2 \ll \frac{yQ}{bS} = \frac{x^\delta Q}{S}.$$

Furthermore, the summation conditions imply $r_1 s \asymp Q/b \asymp r_2 s$, and in particular r_1 and r_2 also satisfy $r_1 \asymp r_2$. In addition, as above, we have $s \asymp Q/(br_1)$ for a given r_1 .

Using this last property to fix the size of s , we have

$$T_2'' \ll \frac{Q}{b} \sum_{\substack{Q/bS \ll r_1 \asymp r_2 \ll yQ/bS}} \sum \frac{1}{r_1} \left(\frac{H_b(br_1)^{1/2}}{(Q[r_1, r_2])^{1/2}} + \frac{(Q[r_1, r_2])^{1/2}}{(br_1)^{1/2}} \right) \\ \sum_{\substack{m_1, m_2 \asymp M \\ r_1^3 m_1 \neq r_2^3 m_2}} (r_1, r_2, m_1 - m_2)^{1/2} \sum_{s \asymp Q/(br_1)} (r_1^3 m_1 - r_2^3 m_2, s)^{1/2}.$$

By Lemma 1.4, the inner sum is $\ll Q/(br_1)$ for all (r_1, r_2, m_1, m_2) , and similarly, we get

$$\sum_{m_1, m_2 \asymp M} (r_1, r_2, m_1 - m_2)^{1/2} \ll M^2 + M(r_1, r_2)^{1/2},$$

so that

$$T_2'' \ll \left(\frac{Q}{b}\right)^2 \sum_{\substack{Q/bS \ll r_1 \asymp r_2 \ll yQ/bS}} \sum \frac{1}{r_1^2} (M^2 + M(r_1, r_2)^{1/2}) \left(\frac{H_b(br_1)^{1/2}}{(Q[r_1, r_2])^{1/2}} + \frac{(Q[r_1, r_2])^{1/2}}{(br_1)^{1/2}} \right).$$

We denote $r = (r_1, r_2)$ and write $r_i = rt_i$, and thus obtain

$$T_2'' \ll \left(\frac{Q}{b}\right)^2 \sum_{r \ll \frac{yQ}{bS}} \frac{M^2 + r^{1/2}M}{r^2} \sum_{\substack{Q/bS \ll t_1 \asymp t_2 \ll yQ/bS}} \frac{1}{t_1^2} \left(\frac{H_b b^{1/2}}{(Qt_2)^{1/2}} + \frac{(Qt_2)^{1/2}}{b^{1/2}} \right) \\ \ll \left(\frac{Q}{b}\right)^2 \sum_{r \ll \frac{yQ}{bS}} \frac{M^2 + r^{1/2}M}{r^2} \sum_{\substack{Q/bS \ll t_2 \ll yQ/bS}} \left(\frac{H_b b^{1/2}}{Q^{1/2} t_2^{3/2}} + \frac{Q^{1/2}}{b^{1/2} t_2^{1/2}} \right) \\ \ll \left(\frac{MQ}{b}\right)^2 \left(\frac{H_b b^{1/2}}{Q^{1/2}} \left(\frac{Q}{bS}\right)^{-1/2} + \frac{Q^{1/2}}{b^{1/2}} \left(\frac{yQ}{bS}\right)^{1/2} \right),$$

as claimed. (Note that it was important to keep track of the condition $r_1 \asymp r_2$.) \square

Proof of Lemma 7.5. If we write $t_i := b_i^\flat$, $b_i = t_i u_i$, then we have $t_i | b$ and $u_i | t_i^\infty$ and

$$\frac{b_1^\flat b_2^\flat b_3^\flat}{(b_1 b_2 b_3)^{1/2} b^3} = \frac{1}{b^3} \prod_{i=1}^3 \frac{t_i^{1/2}}{u_i^{1/2}}$$

and thus we can bound the required series by

$$\sum_{b \geq 1} \frac{1}{b^3} \left(\sum_{t|b} t^{1/2} \sum_{u|t^\infty} \frac{1}{u^{1/2}} \right)^3.$$

Using Euler products, we have

$$\sum_{u|t^\infty} \frac{1}{u^{1/2}} \leq \tau(t)^{O(1)}$$

and thus

$$\sum_{t|b} t^{1/2} \sum_{u|t^\infty} \frac{1}{u^{1/2}} \leq \tau(b)^{O(1)} b^{1/2}$$

and the claim now follows from another Euler product computation. \square

8. AN IMPROVED TYPE I ESTIMATE

In this final section, we prove the remaining Type I estimate from Section 5, namely Theorem 5.1(iii). In Section 5.3, we reduced this estimate to the exponential sum estimate of Theorem 5.8(iii).

8.1. First reduction. The reader is invited to review the definition and notation of Theorem 5.8. We consider the sum

$$\Upsilon := \sum_r \Upsilon_{\ell,r}(b_1, b_2; q_0)$$

of (5.31) for each $1 \leq |\ell| \ll N/R$, where $\Upsilon_{\ell,r}$ was defined in (5.29) and the sum over r is restricted to $r \in \mathcal{D}_I^{(2)}(x^{\delta+o(1)}) \cap [R, 2R]$ (the property that r is doubly densely divisible being part of the assumptions of 5.8(iii)). Our task is to show the bound

$$\Upsilon \ll x^{-\varepsilon} Q^2 R N(q_0, \ell) q_0^{-2}$$

under the hypotheses of Theorem 5.8(iii).

In contrast to the Type I and II estimates of Section 5 (but similarly to the Type III estimate), we will exploit here the average over r , and hence the treatment will combine some features of all the methods used before.

As before, we denote

$$H := x^\varepsilon R Q^2 M^{-1} q_0^{-1}. \quad (8.1)$$

We recall that, from (5.30), we have $H \gg 1$. We begin as in Section 5.6 by exploiting the x^δ -dense divisibility of $q_0 q_1$, which implies the $x^\delta q_0$ -dense divisibility of q_1 by Lemma 2.10(i). Thus we reduce by dyadic decomposition to the proof of

$$\sum_r \Upsilon_{U,V} \ll x^{-\varepsilon}(q_0, \ell) R Q^2 N q_0^{-2} \quad (8.2)$$

(which corresponds to (5.38) with the average over r preserved) where

$$\Upsilon_{U,V} := \sum_{1 \leq |h| \leq H} \sum_{u_1 \asymp U} \sum_{v_1 \asymp V} \sum_{\substack{q_2 \asymp Q/q_0 \\ (u_1 v_1, q_0 q_2) = 1}} \left| \sum_n C(n) \beta(n) \overline{\beta(n + \ell r)} \Phi_\ell(h, n, r, q_0, u_1 v_1, q_2) \right|$$

as in Section 5.6, whenever

$$q_0^{-1} x^{-\delta-2\varepsilon} Q/H \ll U \ll x^{-2\varepsilon} Q/H \quad (8.3)$$

$$q_0^{-1} x^{2\varepsilon} H \ll V \ll x^{\delta+2\varepsilon} H \quad (8.4)$$

$$UV \asymp Q/q_0 \quad (8.5)$$

(which are identical constraints to (5.39), (5.40) and (5.41)), and whenever the parameters (ϖ, δ, σ) satisfy the conditions of Theorem 5.8(iii). As before, u_1, v_1 are understood to be squarefree.

We replace again the modulus by complex numbers c_{r,h,u_1,v_1,q_2} of modulus ≤ 1 , which we may assume to be supported on parameters (r, h, u_1, v_1, q_2) with

$$(u_1 v_1, q_2) = 1$$

and with

$$q_0 u_1 v_1 r, \quad q_0 q_2 r \text{ squarefree.}$$

(These numbers c_{r,h,u_1,v_1,q_2} are unrelated to the exponent c in Theorem 5.1.) We then move the sums over r , n , u_1 and q_2 outside and apply the Cauchy-Schwarz inequality as in the previous sections to obtain

$$\left| \sum_r \Upsilon_{U,V} \right|^2 \leq \Upsilon_1 \Upsilon_2$$

with

$$\Upsilon_1 := \sum_r \sum_{\substack{u_1 \asymp U \\ q_2 \asymp Q/q_0}} \sum_n C(n) |\beta(n)|^2 |\beta(n + \ell r)|^2 \ll (q_0, \ell) \frac{NQRU}{q_0^2}$$

(again as in (5.34)) and

$$\begin{aligned} \Upsilon_2 &:= \sum_r \sum_{\substack{u_1 \asymp U \\ q_2 \asymp Q/q_0}} \sum_n \psi_N(n) C(n) \left| \sum_{v_1 \asymp V} \sum_{1 \leq |h| \leq H} c_{h,r,u_1,v_1,q_2} \Phi_\ell(h, n, r, q_0, u_1 v_1, q_2) \right|^2 \\ &= \sum_r \sum_{\substack{u_1 \asymp U \\ q_2 \asymp Q/q_0}} \sum_{v_1, v_2 \asymp V} \sum_{1 \leq |h_1|, |h_2| \leq H} c_{h_1, r, u_1, v_1, q_2} \overline{c_{h_2, r, u_1, v_2, q_2}} T_{\ell, r}(h_1, h_2, u_1, v_1, v_2, q_2), \end{aligned}$$

where $T_{\ell, r}$ is defined by (5.42) and ψ_N is a smooth coefficient sequence at scale N .

The analysis of Υ_2 will now diverge from Section 5.6. In our setting, the modulus r is doubly $x^{\delta+o(1)}$ -densely divisible. As in the previous section, we will exploit this divisibility to split the average and apply the Cauchy-Schwarz inequality a second time.

Let D be a parameter such that

$$1 \ll D \ll x^\delta R, \quad (8.6)$$

which will be chosen and optimized later. By definition (see Definition 2.1) of doubly densely divisible integers, for each r , there exists a factorization $r = dr_1$ where

$$x^{-\delta} D \ll d \ll D,$$

and where r_1 is $x^{\delta+o(1)}$ -densely divisible (and $(d, r_1) = 1$, since r is squarefree). As before, in the case $D \geq R$ one can simply take $d = r$ and $r_1 = 1$.

We consider the sums

$$\Upsilon_3 := \sum_{\substack{d \asymp \Delta \\ (d, r_1) = 1}} \sum_{1 \leq |h_1|, |h_2| \leq H} \sum_{\substack{v_1, v_2 \asymp V \\ (v_1 v_2, dr_1 q_0 u_1 q_2) = 1}} |T_{\ell, dr_1}(h_1, h_2, u_1, v_1, v_2, q_2)|,$$

with d understood to be squarefree, for all Δ such that

$$\max(1, x^{-\delta} D) \ll \Delta \ll D \quad (8.7)$$

and all (r_1, u_1, q_2) such that

$$r_1 \asymp R/\Delta, \quad u_1 \asymp U, \quad q_2 \asymp Q/q_0, \quad (8.8)$$

and such that $r_1 q_0 u_1 q_2$ is squarefree and the integers r_1 , $q_0 u_1 v_1$, $q_0 u_1 v_2$ and $q_0 q_2$ are $x^{\delta+o(1)}$ -densely divisible.

For a suitable choice of D , we will establish the bound

$$\Upsilon_3 \ll (q_0, \ell) x^{-2\varepsilon} \Delta N V^2 q_0 \quad (8.9)$$

for all such sums. It then follows by dyadic subdivision of the variable d and by trivial summation over r_1 , u_1 and q_2 that

$$\Upsilon_2 \ll (q_0, \ell) x^{-2\varepsilon} N V^2 q_0 \frac{R U Q}{q_0} = (q_0, \ell) x^{-2\varepsilon} N R U V^2 Q,$$

and hence that

$$\left| \sum_r \Upsilon_{U,V} \right|^2 \ll (q_0, \ell)^2 x^{-2\varepsilon} N^2 R^2 \left(\frac{Q}{q_0} \right)^4,$$

which gives the desired result.

We first write $\Upsilon_3 = \Upsilon'_3 + \Upsilon''_3$, where Υ'_3 is the diagonal contribution determined by $h_1 v_2 = h_2 v_1$. The number of quadruples (h_1, v_1, h_2, v_2) satisfying this condition is $\ll HV$ by the divisor bound, and therefore a trivial bound $\ll N$ for $T_{\ell,r}(h_1, h_2, u_1, v_1, v_2, q_2)$ gives

$$\Upsilon'_3 \ll \Delta H N V \ll (q_0, \ell) x^{-2\varepsilon} \Delta N V^2 q_0$$

by (8.4). We now write

$$\Upsilon''_3 = \sum_{\substack{(h_1, v_1, h_2, v_2) \\ h_1 v_2 \neq h_2 v_1}} \Upsilon_4(h_1, v_1, h_2, v_2)$$

where h_1, v_1, h_2, v_2 obey the same constraints as in the definition of Υ_3 , and

$$\Upsilon_4(h_1, v_1, h_2, v_2) := \sum_{\substack{d \asymp \Delta \\ (d, r_1)=1}} |T_{\ell, dr_1}(h_1, h_2, u_1, v_1, v_2, q_2)|.$$

We will shortly establish the following key estimate.

Proposition 8.1. *If $\varepsilon > 0$ is small enough, then we have*

$$\Upsilon_4(h_1, v_1, h_2, v_2) \ll (q_0, \ell) x^{-2\varepsilon} \Delta N H^{-2} q_0 (h_1 v_2 - h_2 v_1, q_0 q_2 r_1 u_1 [v_1, v_2]),$$

if we take

$$D := x^{-5\varepsilon} \frac{N}{H^4} \tag{8.10}$$

and if

$$\begin{cases} \frac{160}{3} \varpi + 16\delta + \frac{34}{9} \sigma < 1 \\ 64\varpi + 18\delta + 2\sigma < 1. \end{cases} \tag{8.11}$$

Assuming this proposition, we obtain

$$\Upsilon''_3 \ll (q_0, \ell) x^{-2\varepsilon} \Delta N V^2 q_0,$$

and hence (8.9), by the following lemma, which will be proved later.

Lemma 8.2. *We have*

$$\sum_{\substack{(h_1, v_1, h_2, v_2) \\ h_1 v_2 \neq h_2 v_1}} (h_1 v_2 - h_2 v_1, q_0 q_2 r_1 u_1 [v_1, v_2]) \ll H^2 V^2.$$

8.2. Reduction of Proposition 8.1 to exponential sums. We now consider a specific choice of parameters r_1, u_1, q_2 and (h_1, v_1, h_2, v_2) , so that $\Upsilon_4 = \Upsilon_4(h_1, v_1, h_2, v_2)$ is a sum with two variables which we write as

$$\Upsilon_4 = \sum_{d \asymp \Delta} \left| \sum_n \psi_N(n) C(n) \Psi(d, n) \right|$$

where $C(n)$ restricts n to the congruence (5.23) and

$$\Psi(d, n) := \Phi_\ell(h_1, n, dr_1, q_0, u_1 v_1, q_2) \overline{\Phi_\ell(h_2, n, dr_1, q_0, u_1 v_2, q_2)}. \quad (8.12)$$

We define D by (8.10), and we first check that this satisfies the constraints (8.6). Indeed, we first have

$$D = x^{-5\varepsilon} \frac{N}{H^4} = \frac{x^{-9\varepsilon} q_0^4 N M^4}{Q^8 R^4} \gg x^{-9\varepsilon - 16\varpi} \frac{R^4}{N^3} \gg x^{1/2 - \sigma - 16\varpi - 4\delta - 21\varepsilon}$$

by (5.2) and (5.12). Under the condition (8.11), this gives $D \gg 1$ if $\varepsilon > 0$ is taken small enough.

Moreover, since $H \gg 1$, we have

$$D = x^{-5\varepsilon} \frac{N}{H^4} \ll x^{-5\varepsilon} N \ll x^{-2\varepsilon + \delta} R \leq x^\delta R.$$

We apply the van der Corput technique with respect to the modulus d . Let

$$L := x^{-\varepsilon} \left\lfloor \frac{N}{\Delta} \right\rfloor. \quad (8.13)$$

Note that from (8.6) and (5.12), it follows that $L \gg x^{-\varepsilon} N R^{-1} \geq 1$ for x sufficiently large.

For any l with $1 \leq l \leq L$, we have

$$\sum_n \psi_N(n) C(n) \Psi(d, n) = \sum_n \psi_N(n + dl) C(n + dl) \Psi(d, n + dl)$$

and therefore

$$|\Upsilon_4| \leq \frac{1}{L} \sum_{d \asymp \Delta} \sum_{n \ll N} \left| \sum_{l=1}^L \psi_N(n + dl) C(n + dl) \Psi(d, n + dl) \right|.$$

By the Cauchy-Schwarz inequality, for some smooth coefficient sequence ψ_Δ at scale Δ , we have

$$|\Upsilon_4|^2 \leq \frac{N\Delta}{L^2} |\Upsilon_5| \quad (8.14)$$

where

$$\Upsilon_5 := \sum_{d \asymp \Delta} \psi_\Delta(d) \sum_n \left| \sum_{l=1}^L \psi_N(n + dl) C(n + dl) \Psi(d, n + dl) \right|^2.$$

Lemma 8.3. *Let*

$$m = q_0 r_1 u_1 [v_1, v_2] q_2.$$

There exist residue classes $\alpha(m)$ and $\beta(m)$, independent of n and l , such that for all n and l we have

$$\Psi(d, n + dl) = \xi(n, d) e_m \left(\frac{\alpha}{d(n + (\beta + l)d)} \right)$$

where $|\xi(n, d)| \leq 1$. Moreover we have $(\alpha, m) = (h_1 v_2 - h_2 v_1, m)$.

Proof. From the definitions (8.12) and (5.29), if $\Psi(d, n)$ does not vanish identically, then we have

$$\begin{aligned} \Psi(d, n+dl) = & e_{dr_1} \left(\frac{a(h_1 - h_2)}{(n+dl)q_0u_1v_1q_2} \right) e_{q_0u_1v_1} \left(\frac{b_1h_1}{(n+dl)dr_1q_2} \right) e_{q_0u_1v_2} \left(-\frac{b_1h_2}{(n+dl)dr_1q_2} \right) \\ & e_{q_2} \left(\frac{b_2h_1}{(n+dl+dlr_1)dr_1q_0u_1v_1} \right) e_{q_2} \left(-\frac{b_2h_2}{(n+dl+dlr_1)dr_1q_0u_1v_2} \right). \end{aligned}$$

By the Chinese Remainder Theorem, the first factor splits into an phase $e_d(\dots)$ that is independent of l , and an expression involving e_{r_1} , which when combined with the other four factors by another application of the Chinese Remainder Theorem, becomes an expression of the type

$$e_m \left(\frac{\alpha}{d(n+ld+\beta d)} \right)$$

for some residue classes α and β modulo m which are independent of l . Furthermore (α, m) is the product of primes p dividing m such that the product of these four factors is trivial, which (since $(q_2, q_0u_1[v_1, v_2]) = 1$) occurs exactly when $p \mid h_2v_1 - h_1v_2$ (recall that b_1 and b_2 are invertible residue classes). \square

Using this lemma, and the notation introduced there, it follows that

$$\begin{aligned} \left| \sum_{l=1}^L \psi_N(n+dl) C(n+dl) \Psi(d, n+dl) \right|^2 & \leq \sum_{1 \leq l_1, l_2 \leq L} \psi_N(n+dl_1) \psi_N(n+dl_2) C(n+dl_1) C(n+dl_2) \\ & \quad e_m \left(\frac{\alpha}{d(n+\beta d+l_1d)} \right) e_m \left(-\frac{\alpha}{d(n+\beta d+l_2d)} \right) \\ & = \sum_{1 \leq l_1, l_2 \leq L} \psi_N(n+dl_1) \psi_N(n+dl_2) e_m \left(\frac{\alpha(l_2-l_1)}{(n+\beta d+l_1d)(n+\beta d+l_2d)} \right), \end{aligned}$$

and therefore, after shifting n by dl_1 , writing $l := l_2 - l_1$, and splitting n, d into residue classes modulo q_0 , that

$$\Upsilon_5 \leq \sum_{n_0, d_0 \in \mathbb{Z}/q_0\mathbb{Z}} C(n_0) \Upsilon_5(n_0, d_0)$$

where

$$\begin{aligned} \Upsilon_5(n_0, d_0) := & \sum_{\substack{|l| \leq L-1 \\ 1 \leq l_1 \leq L}} \sum_{d=d_0} \left| \sum_{(q_0)} \psi_\Delta(d) \right. \\ & \times \sum_{n=n_0} \psi_N(n) \psi_N(n+dl) e_m \left(\frac{\alpha l}{(n+\beta d)(n+(\beta+l)d)} \right) \Big|. \quad (8.15) \end{aligned}$$

Note that m is squarefree. Also, as m is the least common multiple of the $x^{\delta+o(1)}$ -densely divisible quantities r_1 , $q_0u_1v_1$, $q_0u_1v_2$, and q_0q_2 , Lemma 2.10(ii) implies that m is also $x^{\delta+o(1)}$ -densely divisible.

The contribution of $l = 0$ to $\Upsilon_5(n_0, d_0)$ is trivially

$$\ll \frac{NL\Delta}{q_0^2}, \quad (8.16)$$

and this gives a contribution of size

$$\ll \sqrt{(q_0, \ell)} \frac{N\Delta}{\sqrt{q_0 L}}$$

to Υ_4 , as can be seen by summing over the $q_0(q_0, \ell)$ permitted residue classes $(n_0(q_0), d_0(q_0))$. Using (8.10) we have

$$\Delta \ll D = x^{-5\varepsilon} \frac{N}{H^4},$$

and we see from (8.13) that this contribution is certainly

$$\ll (q_0, \ell) x^{-2\varepsilon} \Delta N H^{-2} q_0$$

and hence suitable for Proposition 8.1.

Let $\Upsilon'_5(n_0, d_0)$ (resp. Υ'_5) denote the remaining contribution to $\Upsilon_5(n_0, d_0)$ (resp. Υ_5). It will now suffice to show that

$$\frac{N\Delta}{L^2} |\Upsilon'_5| \ll ((q_0, \ell) x^{-2\varepsilon} \Delta N H^{-2} q_0 (h_1 v_2 - h_2 v_1, q_0 q_2 r_1 u_1 [v_1, v_2]))^2. \quad (8.17)$$

We have

$$\Upsilon'_5(n_0, d_0) = \sum_{1 \leq |l| \leq L-1} \sum_{1 \leq l_1 \leq L} |\Upsilon_6(n_0, d_0)| \quad (8.18)$$

where

$$\begin{aligned} \Upsilon_6(n_0, d_0) &:= \sum_{d=d_0(q_0)} \psi_\Delta(d) \sum_{n=n_0(q_0)} \psi_N(n) \\ &\quad \psi_N(n+dl) e_m \left(\frac{\alpha l}{(n+\beta d)(n+(\beta+l)d)} \right). \end{aligned} \quad (8.19)$$

For given $l \neq 0$ and l_1 , the sum $\Upsilon_6(n_0, d_0)$ over n and d in (8.15) is essentially an incomplete sum in two variables of the type treated in Corollary 6.24. However, before we can apply this result, we must separate the variables n and d in $\psi_N(n+dl)$. As in the previous section, we can do this here using a Taylor expansion.

Let $J \geq 1$ be an integer. Performing a Taylor expansion to order J we have

$$\psi_N(n+dl) = \psi\left(\frac{n+dl}{N}\right) = \sum_{j=0}^J \left(\frac{d}{\Delta}\right)^j \frac{1}{j!} \left(\frac{\Delta l}{N}\right)^j \psi^{(j)}\left(\frac{n}{N}\right) + O(x^{-\varepsilon J})$$

since $dl \ll \Delta L \ll x^{-\varepsilon} N$ by (8.13). We can absorb the factor $(\frac{d}{\Delta})^j$ into ψ_Δ , and after taking J large enough depending on ε , we see that we can express $\Upsilon_6(n_0, d_0)$ as a sum of finitely many sums

$$\Upsilon'_6(n_0, d_0) = \sum_{d=d_0(q_0)} \psi_\Delta(d) \sum_{n=n_1(q_0)} \psi'_N(n) e_m \left(\frac{\alpha l}{(n+\beta d)(n+(\beta+l)d)} \right)$$

for some residue classes $n_1(q_0)$, where ψ_Δ and ψ'_N are coefficient sequences smooth at scales Δ and N respectively, possibly different from the previous ones.

We will prove in Section 8.4 the following exponential sum estimate, using the machinery from Section 6:

Proposition 8.4. *Let m be a y -densely divisible squarefree integer of polynomial size for some $y \geq 1$, let $\Delta, N > 0$ be of polynomial size, and let $\alpha, \beta, \gamma_1, \gamma_2, l \in \mathbb{Z}/m\mathbb{Z}$. Let ψ_Δ, ψ'_N be shifted smooth sequences at scale Δ , and N respectively. Then for any divisor q_0 of m and for all residue classes $d_0 \pmod{q_0}$ and $n_0 \pmod{q_0}$, we have*

$$\left| \sum_{d=d_0 \pmod{q_0}} \sum_{n=n_0 \pmod{q_0}} \psi_\Delta(d) \psi'_N(n) e_m \left(\frac{\alpha l}{(n + \beta d + \gamma_1)(n + (\beta + l)d + \gamma_2)} \right) \right| \\ \ll (\alpha l, m) \left(\frac{N}{q_0 m^{1/2}} + m^{1/2} \right) \left(1 + \left(\frac{\Delta}{q_0} \right)^{1/2} m^{1/6} y^{1/6} + \left(\frac{\Delta}{q_0} \right) m^{-1/2} \right). \quad (8.20)$$

We also have the bound

$$\left| \sum_{d=d_0 \pmod{q_0}} \sum_{n=n_0 \pmod{q_0}} \psi_\Delta(d) \psi'_N(n) e_m \left(\frac{\alpha l}{(n + \beta d + \gamma_1)(n + (\beta + l)d + \gamma_2)} \right) \right| \\ \ll (\alpha l, m) \left(\frac{N}{q_0 m^{1/2}} + m^{1/2} \right) \left(m^{1/2} + \left(\frac{\Delta}{q_0} \right) m^{-1/2} \right). \quad (8.21)$$

Remark 8.5. Suppose $q_0 = 1$ for simplicity. In practice, the dominant term on the right-hand side of (8.21) will be $(\alpha l, m) m^{1/2} \Delta^{1/2} m^{1/6} y^{1/6}$, which in certain regimes improves upon the bound of $((\alpha l, m)^{-1/2} m^{1/2}) \Delta$ that is obtained by completing the sums in the variable n only without exploiting any additional cancellation in the variable d .

Note that if the phase

$$\frac{\alpha l}{(n + \beta d + \gamma_1)(n + (\beta + l)d + \gamma_2)}$$

was of the form $f(d) + g(n)$ for some non-constant rational functions f and g , then the two-dimensional sum would factor into the product of two one-dimensional sums, and then the estimates we claim would basically follow from the one-dimensional bounds in Proposition 4.12. However, no such splitting is available, and so we are forced to use the genuinely multidimensional theory arising from Deligne's proof of the Riemann Hypothesis over finite fields.

Applying Proposition 8.4, we have

$$\Upsilon'_6(n_0, d_0) \ll (\alpha l, m) \left(m^{1/2} + \frac{N/q_0}{m^{1/2}} \right) \left(1 + (\Delta/q_0)^{1/2} m^{1/6} x^{\delta/6} + \frac{\Delta/q_0}{m^{1/2}} \right)$$

as well as

$$\Upsilon'_6(n_0, d_0) \ll (\alpha l, m) \left(m^{1/2} + \frac{N/q_0}{m^{1/2}} \right) \left(m^{1/2} + \frac{\Delta/q_0}{m^{1/2}} \right).$$

Distinguishing the cases $N/q_0 \leq m$ and $N/q_0 > m$, and summing over the finitely many cases of $\Upsilon'_6(n_0, d_0)$ that give $\Upsilon_6(n_0, d_0)$, we see that

$$\Upsilon_6(n_0, d_0) \ll (\alpha l, m) \left\{ m^{1/2} \left(1 + \left(\frac{\Delta}{q_0} \right)^{1/2} m^{1/6} x^{\delta/6} + \frac{\Delta/q_0}{m^{1/2}} \right) + \frac{N/q_0}{m^{1/2}} \left(m^{1/2} + \frac{\Delta/q_0}{m^{1/2}} \right) \right\}.$$

Note that $(\alpha l, m) \leq (\alpha, m)(l, m)$ and hence, summing over l and l_1 in (8.18) (using Lemma 1.4), we get

$$\Upsilon'_5(n_0, d_0) \ll (\alpha, m) L^2 \left\{ m^{1/2} + \left(\frac{\Delta}{q_0} \right)^{1/2} m^{2/3} x^{\delta/6} + \frac{\Delta}{q_0} + \frac{N}{q_0} + \frac{N\Delta}{q_0^2 m} \right\}.$$

Next, summing over the $\leq (q_0, \ell)q_0$ residue classes (n_0, d_0) allowed by the congruence restriction (5.23), we get

$$\Upsilon'_5 \ll (q_0, \ell)(\alpha, m)L^2 \left\{ q_0 m^{1/2} + (q_0 \Delta)^{1/2} m^{2/3} x^{\delta/6} + \Delta + N + \frac{N\Delta}{q_0 m} \right\},$$

and finally by inserting some additional factors of q_0 and (q_0, ℓ) , we derive

$$\begin{aligned} \frac{N\Delta}{L^2} |\Upsilon'_5| &\ll (q_0, \ell)(\alpha, m)N\Delta \left\{ q_0 m^{1/2} + (q_0 \Delta)^{1/2} m^{2/3} x^{\delta/6} + \Delta + N + \frac{N\Delta}{q_0 m} \right\} \\ &\ll (q_0, \ell)^2 (\alpha, m)^2 q_0 N\Delta \left\{ \Delta^{1/2} m^{2/3} x^{\delta/6} + \Delta + N + \frac{N\Delta}{m} \right\}. \end{aligned}$$

In fact, since $\Delta \ll D \ll N$, we see that

$$\frac{N\Delta}{L^2} |\Upsilon'_5| \ll (q_0, \ell)^2 (\alpha, m)^2 q_0 N\Delta \left\{ \Delta^{1/2} m^{2/3} x^{\delta/6} + N + \frac{N\Delta}{m} \right\}.$$

We have $m = q_0 r_1 u_1 [v_1, v_2] q_2$ (see Lemma 8.3) and therefore (using (8.5) and (8.4)) we can bound m from above and below by

$$m \ll q_0 \times \frac{R}{\Delta} \times U \times V^2 \times \frac{Q}{q_0} \asymp \frac{Q^2 R V}{\Delta} \ll x^{\delta+2\varepsilon} \frac{Q^2 R H}{\Delta}$$

and

$$m \gg q_0 \times \frac{R}{\Delta} \times U \times V \times \frac{Q}{q_0} \asymp \frac{Q^2 R}{q_0 \Delta},$$

which leads to

$$\begin{aligned} \frac{N\Delta}{L^2} |\Upsilon'_5| &\ll (q_0, \ell)^2 (\alpha, m)^2 q_0^2 N\Delta \left\{ x^{5\delta/6+4\varepsilon/3} \frac{(Q^2 R H)^{2/3}}{\Delta^{1/6}} + N + \frac{N\Delta^2}{Q^2 R} \right\} \\ &= (q_0, \ell)^2 (\alpha, m)^2 q_0^2 \frac{(N\Delta)^2}{H^4} \left\{ x^{5\delta/6+2\varepsilon} \frac{H^4 (Q^2 R H)^{2/3}}{N\Delta^{7/6}} + \frac{H^4}{\Delta} + \frac{H^4 \Delta}{Q^2 R} \right\} \end{aligned}$$

up to admissible errors. Since

$$\Delta^{-1} \ll \frac{x^\delta}{D} = x^{\delta+5\varepsilon} \frac{H^4}{N}, \quad \Delta \ll D = x^{-5\varepsilon} \frac{N}{H^4},$$

this leads to

$$\frac{N\Delta}{L^2} |\Upsilon'_5| \ll (q_0, \ell)^2 (\alpha, m)^2 q_0^2 \frac{(N\Delta)^2}{H^4} \left\{ x^{2\delta+8\varepsilon} \frac{H^{28/3} Q^{4/3} R^{2/3}}{N^{13/6}} + \frac{x^{\delta+5\varepsilon} H^8}{N} + \frac{x^{-5\varepsilon} N}{Q^2 R} \right\}$$

up to admissible errors. From the assumptions (5.2) and (5.13), we have

$$N \ll x^{1/2} \ll QR,$$

and thus

$$\frac{x^{-5\varepsilon} N}{Q^2 R} \ll x^{-5\varepsilon} Q^{-1} \ll x^{-5\varepsilon}.$$

On the other hand, from the value of H (see (8.1)) we get

$$\begin{aligned} x^{2\delta+8\varepsilon} \frac{H^{28/3} Q^{4/3} R^{2/3}}{N^{13/6}} &\ll x^{2\delta+18\varepsilon} \frac{R^{10} Q^{20}}{M^{28/3} N^{13/6}} \ll x^{-28/3+2\delta+18\varepsilon} R^{10} Q^{20} N^{43/6} \\ \frac{x^{\delta+5\varepsilon} H^8}{N} &\ll x^{\delta+13\varepsilon} \frac{R^8 Q^{16}}{N M^8} \ll x^{-8+\delta+13\varepsilon} N^7 Q^{16} R^8. \end{aligned}$$

Using the other conditions $x^{1/2} \ll QR \ll x^{1/2+2\varpi}$, and

$$R \gg x^{-3\varepsilon-\delta} N, \quad N \gg x^{1/2-\sigma}$$

these quantities are in turn bounded respectively by

$$\begin{aligned} x^{2\delta+8\varepsilon} \frac{H^{28/3} Q^{4/3} R^{2/3}}{N^{13/6}} &\leq x^{2/3+2\delta+40\varpi+18\varepsilon} \frac{N^{43/6}}{R^{10}} \ll x^{2/3+12\delta+40\varpi-17/6(1/2-\sigma)+48\varepsilon} \\ \frac{x^{\delta+5\varepsilon} H^8}{N} &\leq x^{\delta+32\varpi+13\varepsilon} \frac{N^7}{R^8} \ll x^{9\delta+32\varpi+37\varepsilon-(1/2-\sigma)}. \end{aligned}$$

Thus, by taking $\varepsilon > 0$ small enough, we obtain (8.17) (and hence Proposition 8.1) provided

$$\begin{cases} \frac{2}{3} + 12\delta + 40\varpi - \frac{17}{6}(\frac{1}{2} - \sigma) < 0 \\ 9\delta + 32\varpi - (\frac{1}{2} - \sigma) < 0. \end{cases} \Leftrightarrow \begin{cases} \frac{160}{3}\varpi + 16\delta + \frac{34}{9}\sigma < 1 \\ 64\varpi + 18\delta + 2\sigma < 1. \end{cases}$$

These are exactly the conditions claimed in Proposition 8.1.

8.3. Proof of Lemma 8.2. This is a bit more complicated than the corresponding lemmas in Sections 5.4-5.6 because the quantity $m = q_0 q_2 r_1 u_1 [v_1, v_2]$ depends also on v_1 and v_2 .

We let $w := q_0 q_2 r_1 u_1$, so that $m = w[v_1, v_2]$ and w is independent of (h_1, h_2, v_1, v_2) and coprime with $[v_1, v_2]$.

Since $(w, [v_1, v_2]) = 1$, we have

$$(h_1 v_2 - h_2 v_1, w[v_1, v_2]) = \sum_{\substack{d|h_1 v_2 - h_2 v_1 \\ d|w[v_1, v_2]}} \varphi(d) \leq \sum_{d|w} d \sum_{\substack{e|[v_1, v_2] \\ de|h_1 v_2 - h_2 v_1}} e,$$

and therefore

$$\begin{aligned} \sum_{\substack{(h_1, v_1, h_2, v_2) \\ h_1 v_2 \neq h_2 v_1}} (h_1 v_2 - h_2 v_1, q_0 q_2 r_1 u_1 [v_1, v_2]) &\leq \sum_{\substack{(h_1, v_1, h_2, v_2) \\ h_1 v_2 \neq h_2 v_1}} \sum_{d|w} d \sum_{\substack{e|[v_1, v_2] \\ de|h_1 v_2 - h_2 v_1}} e \\ &\leq \sum_{d|w} d \sum_{\substack{(d, e)=1 \\ e \ll V^2 \\ e \text{ squarefree}}} e \sum_{\substack{([v_1, v_2], w)=1 \\ de|h_1 v_2 - h_2 v_1 \\ e|[v_1, v_2] \\ h_1 v_2 \neq h_2 v_1}} 1. \end{aligned}$$

The variable d is unrelated to the modulus d appearing previously in this section.

Let d, e be integers occurring in the outer sums, and (h_1, h_2, v_1, v_2) satisfying the other summation conditions. Then e is squarefree, and since $e \mid [v_1, v_2]$ and $e \mid h_1 v_2 - h_2 v_1$, any prime dividing e must divide one of (v_1, v_2) , (h_1, v_1) or (h_2, v_2) (if it does not divide both v_1 and v_2 , it is coprime to one of them, and $h_1 v_2 - h_2 v_1 = 0 \pmod{p}$ gives one of the other divisibilities). Thus if we factor $e = e_1 e_2 e_3$ where

$$e_1 := \prod_{\substack{p|e \\ p|v_1 \\ p \nmid v_2}} p, \quad e_2 := \prod_{\substack{p|e \\ p \nmid v_1 \\ p|v_2}} p, \quad e_3 := \prod_{\substack{p|e \\ p|(v_1, v_2)}} p,$$

then these are coprime and we have

$$e_1 \mid h_1, \quad e_2 \mid h_2, \quad e_1 e_3 \mid v_1, \quad e_2 e_3 \mid v_2.$$

We write

$$h_1 = e_1 \lambda_1, \quad h_2 = e_2 \lambda_2, \quad v_1 = e_1 e_3 \nu_1, \quad v_2 = e_2 e_3 \nu_2.$$

Then we get

$$h_1 v_2 - h_2 v_1 = e(\lambda_1 \nu_2 - \lambda_2 \nu_1),$$

and since $de \mid h_1 v_2 - h_2 v_1$, it follows that $d \mid \lambda_1 \nu_2 - \lambda_2 \nu_1$.

Now fix some $e \ll V^2$. For each choice of factorization $e = e_1 e_2 e_3$, the number of pairs $(\lambda_1 \nu_2, \lambda_2 \nu_1)$ that can be associated to this factorization as above for some quadruple (h_1, h_2, v_1, v_2) is $\ll (HV/e)^2/d$, since each product $\lambda_1 \nu_2, \lambda_2 \nu_1$ is $\ll HV/e$, and d divides the difference. By the divisor bound, this gives $\ll (HV)^2/de^2$ for the number of quadruples (h_1, h_2, v_1, v_2) . Summing over $d \mid w$ and e , we get a total bound

$$\ll (HV)^2 \tau(w) \sum_{e \ll V^2} e^{-1} \ll H^2 V^2,$$

as desired.

8.4. Proof of Proposition 8.4. It remains to establish Proposition 8.4. We begin with the special case when $e = 1$ and $(\alpha l, m) = 1$. For simplicity, we denote

$$f(n, d) = \frac{\alpha l}{(n + \beta d + \gamma_1)(n + (\beta + l)d + \gamma_2)}.$$

By completion of the sum over n (see Lemma 4.9(i)), we have

$$\begin{aligned} \sum_d \sum_n \psi_\Delta(d) \psi_N(n) e_m(f(n, d)) &\ll \left(\frac{N}{m} + 1 \right) \sup_{h \in \mathbb{Z}/m\mathbb{Z}} \left| \sum_d \psi_\Delta(d) \sum_{n \in \mathbb{Z}/m\mathbb{Z}} e_m(f(n, d) + hn) \right| \\ &= \left(\frac{N}{\sqrt{m}} + \sqrt{m} \right) \sup_{h \in \mathbb{Z}/m\mathbb{Z}} \left| \sum_d \psi_\Delta(d) K_h(d; m) \right|, \end{aligned} \quad (8.22)$$

where, for each $h \in \mathbb{Z}/m\mathbb{Z}$, we define

$$K_h(d; m) := \frac{1}{\sqrt{m}} \sum_{n \in \mathbb{Z}/m\mathbb{Z}} e_m(f(n, d) + hn).$$

By the first part of Corollary 6.24 (i.e., (6.23)), we get

$$\left| \sum_d \psi_\Delta(d) K_h(d; m) \right| \ll m^{1/2} + \Delta m^{-1/2}, \quad (8.23)$$

and this combined with (8.22) implies the second bound (8.21) (in the case $e = 1$, $(\alpha l, m) = 1$, that is). Furthermore, it also implies the first bound (8.20) for $\Delta > m^{2/3} y^{-1/3}$.

In addition, from the Chinese Remainder Theorem (Lemma 4.4) and (6.16), we deduce the pointwise bound

$$|K_h(d, m)| \ll 1 \quad (8.24)$$

which implies the trivial bound

$$\left| \sum_d \psi_\Delta(d) K_h(d; m) \right| \ll 1 + \Delta,$$

which gives (8.20) for $\Delta \leq m^{1/3} y^{1/3}$. Thus we can assume that

$$m^{1/3} y^{1/3} \leq \Delta \leq m^{2/3} y^{-1/3} \leq m.$$

We can then use the y -dense divisibility of m to factor $m = m_1 m_2$ where

$$\begin{aligned} y^{-2/3} m^{1/3} &\leq m_1 \leq y^{1/3} m^{1/3} \\ y^{-1/3} m^{2/3} &\leq m_2 \leq y^{2/3} m^{2/3}. \end{aligned}$$

Now the second part of Corollary 6.24 (i.e., (6.24)) gives

$$\left| \sum_d \psi_\Delta(d) K_h(d; m) \right| \ll \Delta^{1/2} m_1^{1/2} + \Delta^{1/2} m_2^{1/4} \ll \Delta^{1/2} m^{1/6} y^{1/6},$$

which together with (8.22) gives (8.20).

This finishes the proof of Proposition 8.4 for the special case $e = 1$ and $(\alpha l, m) = 1$. The extension to a divisor $e \mid m$ is done exactly as in the proof of Corollary 4.16 in Section 4.

We now reduce to the case $(\alpha l, m) = 1$. Let

$$\begin{aligned} m' &:= m/(\alpha l, m) \\ y' &:= y(\alpha l, m) \\ \alpha' &:= \alpha/(\alpha l, m) = \frac{\alpha/(\alpha, m)}{(\alpha l, m)/(\alpha, m)}, \end{aligned}$$

where one computes the reciprocal of $(\alpha l, m)/(\alpha, m)$ inside $\mathbb{Z}/m'\mathbb{Z}$, so that α' is viewed as an element of $\mathbb{Z}/m'\mathbb{Z}$. The integer m' is y' -densely divisible by Lemma 2.10 (ii), and it is also squarefree, and of polynomial size. We have $(\alpha' l, m') = 1$, and furthermore

$$\begin{aligned} \sum_d \sum_n \psi_\Delta(d) \psi_N(n) e_m(f(n, d)) &= \sum_d \sum_n \psi_\Delta(d) \psi_N(n) e_{m'}(f'(n, d)) \\ &\quad \times \prod_{p \mid (\alpha l, m)} (1 - \mathbf{1}_{p \mid (n + \beta d + \gamma_1)(n + (\beta + l)d + \gamma_2)}) \end{aligned}$$

where

$$f'(n, d) = \frac{\alpha' l}{(n + \beta d + \gamma_1)(n + (\beta + l)d + \gamma_2)}$$

(here we use the convention explained at the end of Section 4.1 that leads to $e_p(\alpha x) = 1$ if p is prime, $\alpha = 0 \pmod{p}$ and $x = +\infty \in \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$).

Denote

$$g(n, d) = (n + \beta d + \gamma_1)(n + (\beta + l)d + \gamma_2).$$

Then, expanding the product (as in inclusion-exclusion), we get

$$\sum_d \sum_n \psi_\Delta(d) \psi_N(n) e_m(f(n, d)) = \sum_{\delta \mid (\alpha l, m)} \mu(\delta) \sum_{\substack{d, n \\ \delta \mid g(n, d)}} \psi_\Delta(d) \psi_N(n) e_{m'}(f'(n, d))$$

(this usage of δ is unrelated to prior usages of δ in this section). Splitting the sum over n and d in residue classes modulo δ , this sum is then equal to

$$\sum_{\delta \mid (\alpha l, m)} \mu(\delta) \sum_{\substack{(d_0, n_0) \in (\mathbb{Z}/\delta\mathbb{Z})^2 \\ g(n_0, d_0) \equiv 0 \pmod{\delta}}} \sum_{n \equiv n_0 \pmod{\delta}} \sum_{d \equiv d_0 \pmod{\delta}} \psi_\Delta(d) \psi_N(n) e_{m'}(f'(n, d)).$$

For each choice of (n_0, d_0) , we can apply the case previously proved of Proposition 8.4 to deduce

$$\sum_{n=n_0} \sum_{(n) \mid d=d_0} \psi_{\Delta}(d) \psi_N(n) e_{m'}(f'(n, d)) \ll \left(\sqrt{m'} + \frac{N}{\delta \sqrt{m'}} \right) \left(1 + \frac{\Delta^{1/2}}{\delta^{1/2}} (m' y')^{1/6} + \frac{\Delta}{\delta \sqrt{m'}} \right)$$

and

$$\sum_{n=n_0} \sum_{(n) \mid d=d_0} \psi_{\Delta}(d) \psi_N(n) e_{m'}(f'(n, d)) \ll \left(\sqrt{m'} + \frac{N}{\delta \sqrt{m'}} \right) \left(\sqrt{m'} + \frac{\Delta}{\delta \sqrt{m'}} \right).$$

Moreover, by the Chinese Remainder Theorem, there are $\ll \delta$ solutions $(n_0, d_0) \in (\mathbb{Z}/\delta\mathbb{Z})^2$ of $g(n_0, d_0) = 0 \pmod{\delta}$, and there we find

$$\sum_d \sum_n \psi_{\Delta}(d) \psi_N(n) e_m(f(n, d)) \ll \sum_{\delta | (\alpha l, m)} \delta \left(\sqrt{m'} + \frac{N}{\delta \sqrt{m'}} \right) \left(1 + \frac{\Delta^{1/2}}{\delta^{1/2}} (m' y')^{1/6} + \frac{\Delta}{\delta \sqrt{m'}} \right)$$

and

$$\sum_d \sum_n \psi_{\Delta}(d) \psi_N(n) e_m(f(n, d)) \ll \sum_{\delta | (\alpha l, m)} \delta \left(\sqrt{m'} + \frac{N}{\delta \sqrt{m'}} \right) \left(\sqrt{m'} + \frac{\Delta}{\delta \sqrt{m'}} \right).$$

It is now elementary to check that these give the bounds of Proposition 8.4 (note that $m' y' = m y$).

REFERENCES

- [1] M. B. Barban, P. P. Vehov, *Summation of multiplicative functions of polynomials*, Mat. Zametki, 5 (1969), 669–680.
- [2] E. Bombieri, *Counting points on curves over finite fields (d'après Stepanov)*, Sémin. Bourbaki, Exposé 430 (1973).
- [3] E. Bombieri, J. Friedlander, H. Iwaniec, *Primes in arithmetic progressions to large moduli*, Acta Math. 156 (1986), no. 3–4, 203–251.
- [4] E. Bombieri, J. Friedlander, H. Iwaniec, *Primes in arithmetic progressions to large moduli. II*, Math. Ann. 277 (1987), no. 3, 361–393.
- [5] E. Bombieri, J. Friedlander, H. Iwaniec, *Primes in arithmetic progressions to large moduli. III*, J. Amer. Math. Soc. 2 (1989), no. 2, 215–224.
- [6] T. Cochrane, C. Pinner, *Using Stepanov's method for exponential sums involving rational functions*, J. Number Theory 116 (2006), no. 2, 270–292.
- [7] P. Deligne, *Cohomologie étale. Séminaire de Géométrie Algébrique du Bois-Marie SGA 41/2*. Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier. Lecture Notes in Mathematics, Vol. 569. Springer-Verlag, Berlin-New York, 1977.
- [8] P. Deligne, *La conjecture de Weil. I*, Publications Mathématiques de l'IHÉS 43 (1974), 273–307.
- [9] P. Deligne, *La conjecture de Weil. II*, Publications Mathématiques de l'IHÉS 52 (1980), 137–252.
- [10] É. Fouvry, *Autour du théorème de Bombieri-Vinogradov*, Acta Math. 152 (1984), no. 3–4, 219–244.
- [11] É. Fouvry, *Sur le problème des diviseurs de Titchmarsh*, J. Reine Angew. Math. **357** (1985), 51–76.
- [12] É. Fouvry, H. Iwaniec, *On a theorem of Bombieri-Vinogradov type*, Mathematika 27 (1980), no. 2, 135–152 (1981).
- [13] É. Fouvry, H. Iwaniec, *Primes in arithmetic progressions*, Acta Arith. 42 (1983), no. 2, 197–218.
- [14] É. Fouvry, H. Iwaniec, *The divisor function over arithmetic progressions*. (With an appendix by Nicholas Katz.) Acta Arith. 61 (1992), no. 3, 271–287.
- [15] É. Fouvry, E. Kowalski, Ph. Michel, *Algebraic twists of modular forms and Hecke orbits*, preprint [arXiv:1207.0617](https://arxiv.org/abs/1207.0617), (2012).
- [16] É. Fouvry, E. Kowalski, Ph. Michel, *On the exponent of distribution of the ternary divisor function*, to appear, Mathematika; [arXiv:1304.3199](https://arxiv.org/abs/1304.3199), (2013).

- [17] É. Fouvry, E. Kowalski, Ph. Michel, *An inverse theorem for Gowers norms of trace functions over prime fields*, Proc. Cambridge Phil. Math. Soc. 155 (2013), 277–295.
- [18] É. Fouvry, E. Kowalski, Ph. Michel, *The sliding sum method for short exponential sums*, preprint (2013).
- [19] É. Fouvry, E. Kowalski, Ph. Michel, *On the conductor of cohomological transforms*, preprint (2013).
- [20] É. Fouvry, E. Kowalski, Ph. Michel, *Trace functions over finite fields and their applications*, Colloquium De Giorgi, Colloquia (Scuola Normale Superiore), to appear.
- [21] J. Friedlander, H. Iwaniec, *Incomplete Kloosterman sums and a divisor problem*, With an appendix by Bryan J. Birch and Enrico Bombieri. Ann. of Math. (2) 121 (1985), no. 2, 319–350.
- [22] P.X. Gallagher: *Bombieri’s mean value theorem*, Mathematika 15 (1968), 1–6.
- [23] D. Goldston, J. Pintz, C. Yıldırım, *Primes in tuples. I*, Ann. of Math. 170 (2009), no. 2, 819–862.
- [24] S. W. Graham, C. J. Ringrose, *Lower bounds for least quadratic nonresidues*, Analytic number theory (Allerton Park, IL, 1989), 269–309, Progr. Math., 85, Birkhäuser Boston, Boston, MA, 1990.
- [25] D. R. Heath-Brown, *Hybrid bounds for Dirichlet L -functions*, Invent. Math. 47 (1978), no. 2, 149–170.
- [26] D. R. Heath-Brown, *Prime numbers in short intervals and a generalized Vaughan identity*, Canad. J. Math. 34 (1982), no. 6, 1365–1377.
- [27] D. R. Heath-Brown, *The divisor function $d_3(n)$ in arithmetic progressions*, Acta Arith. 47 (1986), no. 1, 29–56.
- [28] D. R. Heath-Brown, *The largest prime factor of $X^3 + 2$* , Proc. London Math. Soc. (3) 82 (2001), no. 3, 554–596.
- [29] H. Iwaniec, *A new form of the error term in the linear sieve*, Acta Arith., 37 (1980), 307–320.
- [30] H. Iwaniec, E. Kowalski, Analytic Number Theory, American Mathematical Society Colloquium Publications Vol. 53, 2004.
- [31] N. M. Katz, *Sommes exponentielles*, Astérisque 79 (1980).
- [32] N. M. Katz, *Gauss sums, Kloosterman sums and monodromy groups*, Annals of Math. Studies 116, Princeton Univ. Press, 1988.
- [33] N. M. Katz, *L -functions and monodromy: four lectures on Weil II*, Adv. Math. 160 (2001), no. 1, 81–132.
- [34] H. D. Kloosterman, *On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$* , Acta Mathematica 49 (1926), 407–464.
- [35] E. Kowalski, *Some aspects and applications of the Riemann Hypothesis over finite fields*, Proceedings of the Riemann International School of Mathematics Conference (April 2009), Milan Journal of Mathematics 78 (2010), 179–220.
- [36] G. Laumon, *Transformation de Fourier, constantes d’équations fonctionnelles et conjecture de Weil*, Publ. Math. IHÉS, 65 (1987), 131–210.
- [37] Yu. V. Linnik, *The dispersion method in binary additive problems*, AMS, 1963.
- [38] J. Maynard, *Small gaps between primes*, preprint.
- [39] Ph. Michel, *Minorations de sommes d’exponentielles*, Duke Math. J., 95, 2, pp. 227–240 (1998).
- [40] H. L. Montgomery, R. C. Vaughan, *Multiplicative Number Theory I. Classical Theory*, Cambridge studies in advanced mathematics, 2007.
- [41] L. J. Mordell, *On a sum analogous to a Gauss’s sum*, Quart. J. Math. Oxford Ser. 3 (1932), 161–167.
- [42] Y. Motohashi, *An induction principle for the generalization of Bombieri’s Prime Number Theorem*, Proc. Japan Acad. 52 (1976), 273–275.
- [43] Y. Motohashi, J. Pintz, *A smoothed GPY sieve*, Bull. Lond. Math. Soc. 40 (2008), no. 2, 298–310.
- [44] G. I. Perel’muter, *Estimate of a sum along an algebraic curve*, Mat. Zametki 5 (1969), 373–380.
- [45] J. Pintz, *A note on bounded gaps between primes*, preprint.
- [46] D.H.J. Polymath: *New equidistribution estimates of Zhang type, and bounded gaps between primes*, arXiv:1402.0811v2.
- [47] D.H.J. Polymath: *Variants of the Selberg sieve, and bounded intervals containing many primes*, preprint (2014), arXiv:1407.4897

- [48] P. Shiu, *A Brun-Titchmarsh theorem for multiplicative functions*, J. Reine Angew. Math. 313 (1980), 161–170.
- [49] H. Siebert, *Einige Analoga zum Satz von Siegel-Walfisz*, in: Zahlentheorie (Tagung, Math. Forschungsinst., Oberwolfach, 1970), Bibliographisches Inst., Mannheim, 1971, 173–184.
- [50] R. C. Vaughan, *Sommes trigonométriques sur les nombres premiers*, C. R. Acad. Sci. Paris Sér. A 285 (1977), 981–983.
- [51] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind. 1041, Hermann, 1948.
- [52] Y. Zhang, *Bounded gaps between primes*, to appear, Ann. of Math.

[HTTP://MICHAELNIELSEN.ORG/POLYMATH1/INDEX.PHP](http://MICHAELNIELSEN.ORG/POLYMATH1/INDEX.PHP)